Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate
CyberNotes

Issue #2003-12 *June 16, 2003*

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between May 15 and June 13, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Aladdin Enterprises[1,2, 3]	Unix	Ghostscript 5.10.10, 5.10.15, 5.10.16, 5.50, 5.50.8, 6.51-6.53, 7.0 4-7.0 6	A vulnerability exists when Ghostscript is used to process specially formatted PS files, which could let a malicious user execute arbitrary commands.	Upgrade available at: http://prdownloads.sourceforge.net/ghostscript/ghostscript-7.07.tar.gz?download **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **OpenPKG:** ftp.openpkg.org **RedHat:** ftp://updates.redhat.com/ **Sun:** ftp://ftp.cobalt.sun.com/pub/products/sunlinux/5.0/en/updates/i3	GhostScript Arbitrary Command Execution CVE Name: CAN-2003-0354	**High**	Bug discussed in newsgroups and websites.

[1] Red Hat Security Advisory, RHSA-2003:181-01, May 30, 2003,

[2] OpenPKG Security Advisory, OpenPKG-SA-2003.030, June 3, 2003.

[3] Mandrake Linux Security Update Advisory, MDKSA-2003:065, June 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
AMAX Information Technologies Inc.[4] ***Exploit script published***[5]	**Windows**	**Magic Winmail Server 2.3**	**A remote Denial of Service vulnerability exists due to insufficient validation of user-supplied input to the 'USER' and 'PASS' commands.**	**No workaround or patch available at time of publishing.**	**Magic Winmail Remote Denial of Service**	**Low**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***
Apple[6]	MacOS X 10.2-10.2.6	MacOS X Server 10.2-10.2.6	A vulnerability exists because plaintext passwords are leaked in a network that uses Kerberos, which could let a malicious user obtain unauthorized access.	Upgrade available at: http://www.info.apple.com/kbnum/n120223	Mac OS X Server Authentication ClearText Passwords CVE Name: CAN-2003-0378	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Apple[7]	MacOS X 10.2x	MacOS X Server 10.2-10.2.6	A vulnerability exists in the AFP server when the application is used to reshare a Network File System (NFS) mount, which could let a remote malicious user execute corrupt arbitrary files.	Upgrade available at: http://www.info.apple.com/kbnum/n120223	Apple AFP Server Arbitrary File Corruption CVE Name: CAN-2003-0379	**High**	Bug discussed in newsgroups and websites.
ArGoSoft[8]	Windows NT 4.0/2000, XP	Mail Server FreeWare 1.8.3 .5	A remote Denial of Service vulnerability exists when a malicious user submits multiple GET requests.	No workaround or patch available at time of publishing.	ArGoSoft Mail Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[4] Damage Hacking Group Security Advisory, May 23, 2003.
[5] SecurityFocus, June 11, 2003.
[6] Apple Article ID, 120223, June 13, 2003.
[7] Apple Security Update, 120223, June 13, 2003.
[8] Tripbit Security Advisory, TA-2003-06, June 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
AStArt Technologies[9] ***RedHat issues advisory***[10] ***More advisories issued***[11, 12] ***More advisories issued***[13, 14]	**Unix**	**LPRng 3.8.10 .1**	**A vulnerability exists in the 'psbanner' filter because temporary files for debugging purposes are created insecurely, which could let a malicious user obtain elevated privileges.**	**Debian:** **http://security.debian.org/pool/updates/main/l/lprng/** ***RedHat:*** **ftp://updates.redhat.com** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***Immunix:*** **http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/LPRng-3.6.24-2_imnx_1.i386.rpm** ***YellowDog:*** **ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/**	**LPRng 'PSBanner' Insecure Temporary File Creation** **CVE Name: CAN-2003-0136**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
atftpd[15]	Unix	atftpd 0.6.0, 0.6.1.1	A buffer overflow vulnerability exists due to insufficient bounds checking when handling filenames of excessive length, which could let a remote malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/a/atftp/	ATFTPD Remote Filename Length Buffer Overrun CVE Name: CAN-2003-0380	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Atrium Software[16]	Multiple	MERCUR Mailserver 4.2, SP1&SP2	A buffer overflow vulnerability exists in the IMAP process, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Mercur Mailserver IMAP Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Biz-Design, Inc.[17]	Windows, Unix	ImageFolio 2.23, 2.24, 2.26, 2.27, 3.0.1, 3.1	A Directory Traversal vulnerability exists in the 'admin.cgi' script, which could let a remote malicious user obtain sensitive information.	Patch available at: http://www.imagefolio.com/ubb/Forum25/HTML/000019.html	ImageFolio 'Admin.CGI' Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Code-Crafters[18]	Windows	Ability Mail Server 1.0.9	A vulnerability exists because usernames and passwords are stored in plaintext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Ability Mail Server Plaintext Password Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[9] Debian Security Advisory, DSA 285-1, April 14, 2003.
[10] Red Hat Security Advisory, RHSA-2003:142-01, April 24, 2003.
[11] Mandrake Linux Security Update Advisory, MDKSA-2003:060, May 21, 2003.
[12] RedHat Security Advisory, RHSA-2003:150-04, May 22, 2003.
[13] Yellow Dog Linux Security Announcement, YDU-20030602-5, June 2, 2003.
[14] Immunix Secured OS Security Advisory, IMNX-2003-7+-013-01, June 6, 2003.
[15] Debian Security Advisory, DSA 314-1, June 11, 2003.
[16] Secunia Security Advisory, May 9, 2003.
[17] Bugtraq, June 5, 2003.
[18] SecurityTracker Alert ID, 1006915, June 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Computer Associates[19]	Multiple	Unicenter Asset Manager	A vulnerability exists because password information is stored in a way that may be easily recovered, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Unicenter Asset Manager Stored Data Decryption	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Computer Associates[20]	Multiple	Unicenter TNG 2.1, 2.4, 2.4.2	Several vulnerabilities exist: a vulnerability exists in the 'file_upload.pl' script, which could let a remote malicious user execute arbitrary commands; a vulnerability exists in the 'pdmcgi.exe' utility, which could let a malicious user obtain unauthorized access; a vulnerability exists in 'pdm_cgireport.exe' utility, which could let a malicious user obtain sensitive information; and a vulnerability exists in the 'pdmcgi.exe' utility, which could let an unauthorized malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Unicenter TNG Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Crob Software Studio[21]	Windows	Crob FTP Server 2.50.4	A vulnerability exists in the 'USER' command due to invalid format specifiers, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Crob FTP Server Remote Username Format String	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Denis Verreault[22]	Windows	Aiglon web server 2.0	A vulnerability exists because installation path details may be disclosed when a malformed HTTP request is submitted, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Aiglon Web Server Installation Path Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[19] Bugtraq, June 4, 2003.
[20] Bugtraq, June 4, 2003.
[21] Securiteam, June 2, 2003.
[22] SecurityTracker Alert ID, 1006953, June 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Easy Software Products[23] ***Vendors release patches***[24, 25,26, 27, 28, 29,]	**Unix**	**CUPS 1.1.17, 1.1.18**	**A remote Denial of Service vulnerability exists due to an insufficient time-out process for malicious HTTP requests.**	**Patch available at:** **http://www.cups.org/strfiles/75/cups-1.1.18-str75.patchv2** ***Debian:*** **http://security.debian.org/pool/updates/main/c/cupsys/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***RedHat:*** **ftp://updates.redhat.com** ***Slackware:*** **ftp://ftp.slackware.com/pub/slackware/** ***SuSE:*** **ftp://ftp.suse.com/pub/suse/** ***YellowDog:*** **ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/**	**CUPS Time-out Remote Denial of Service**	**Low**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Eterm[30] ***Debian issues patches***[31]	**Unix**	**Eterm 0.9.1, 0.9.2**	**A buffer overflow vulnerability exists in the 'PATH_ENV' variable due to insufficient bounds checking, which could let a malicious user execute arbitrary code.**	***Debian:*** **http://security.debian.org/pool/updates/main/e/eterm/**	**Eterm Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***

[23] Turbolinux Security Advisory, TLSA-2003-33, May 20, 2003.
[24] Red Hat Security Advisory, RHSA-2003:171-01, May 27, 2003.
[25] Mandrake Linux Security Update Advisory, MDKSA-2003:062:, May 29, 2003.
[26] Slackware Security Advisory, May 29, 2003.
[27] Yellow Dog Linux Security Announcement, YDU-20030602-3, June 2, 2003.
[28] SuSE Security Announcement, SuSE-SA:2003:028, June 6, 2003.
[29] Debian Security Advisor, DSA 317-1, June 11, 2003.
[30] SecurityFocus, May 27, 2003.
[31] Debian Security Advisory, DSA 309-2, June 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ethereal Group[32]	Windows 95/98/ME/ NT 4.0/2000, XP, Unix	Ethereal 0.9.0-0.9.12	Multiple vulnerabilities exist: a vulnerability exists in the DCERPC dissector when decoding certain NDR strings, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a vulnerability exists in the SPNEGO dissector when parsing certain ASN.1 codes, which could let a remote malicious user cause a Denial of Service; a buffer overflow vulnerability exists in the OSI dissector when handling bad IPv4 or IPv6 prefix lengths due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the BGP, WTP, DNS, 802.11, ISAKMP, WSP, CLNP, ISIS, and RMI dissectors because certain strings are not properly handled, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and a vulnerability exists in the tvb_get_nstringz0() routine because a zero-length buffer size is incorrectly handled, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Upgrade available at: http://www.ethereal.com/distribution/ethereal-0.9.13.tar.gz	Ethereal Multiple Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Fastraq[33]	Windows NT 4.0	Mailtraq 2.2	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exits in the 'browse.asp' script due to insufficient sanitization of HTTP requests, which could let a malicious user execute arbitrary code; a vulnerability exists due to insufficient sanitization of HTTP requests, which could let a malicious user obtain ASP script files' source code; and a path disclosure vulnerability exists due to insufficient sanitization of HTTP requests for non-existent resources, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Mailtraq Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. for the Cross-Site Scripting and utility path disclosure vulnerabilities. The ASP Script vulnerability can be exploited via a web browser.

[32] Ethereal Advisory, enpa-sa-00010, June 11, 2003.
[33] Securiteam, June 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Felipe et al Bergo[34]	Unix	gps 0.9.4, 0.10.1-0.10.3, 1.0.0	Several vulnerabilities exists in the graphical process monitoring utility, which could let a local/remote malicious user cause a Denial of Service or obtain unauthorized access.	Upgrade available at: ftp://ftp.seul.org/pub/gps/gps-1.1.0.tar.gz **Debian:** http://security.debian.org/pool/updates/main/g/gps/	Multiple GPS Local & Remote Vulnerabilities	Low/ Medium (Medium if unauthorized access can be obtained)	Bug discussed in newsgroups and websites.
file[35, 36, 37] ***More updates issued[38, 39, 40, 41]*** ***More updates issued[42]***	**Unix**	**file 3.28, 3.30, 3.32-3.37, 3.39, 3.40**	**A buffer overflow vulnerability exists in the file utility ELF parsing routines, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code.**	**Upgrade available at:** ftp://ftp.gw.com/mirrors/pub/unix/file/file-3.41.tar.gz **RedHat:** **ftp://updates.redhat.com/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **OpenPKG:** **ftp://ftp.openpkg.org/** ***NetBSD:*** **ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-003.txt.asc** ***Debian:*** **http://security.debian.org/pool/updates/main/f/file/** ***Trustix:*** **http://www.trustix.net/pub/Trustix/updates/** ***SuSE:*** **ftp://ftp.suse.com/pub/suse** ***Immunix:*** **http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/file-3.30-7_imnx_3.41_1.i386.rpm**	**File ELF Routine Buffer Overflow** **CVE Name: CAN-2003-0102**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Exploit script has been published.**

[34] Debian Security Advisory, DSA 307-1, May 27, 2003.
[35] OpenPKG Security Advisory, OpenPKG-SA-2003.017, March 4, 2 003.
[36] Mandrake Linux Security Update Advisory, MDKSA-2003:030, March 6, 2003.
[37] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:086-07, March 7, 2003.
[38] NetBSD Security Advisory, 2003-003, March 12, 2003.
[39] Debian Security Advisory, DSA-260-1, March 13, 2003.
[40] Trustix Secure Linux Bugfix Advisory, TSL-2003-0006, March 18, 2003.
[41] SuSE Security Announcement, SuSE-SA:2003:017, March 21, 2003.
[42] Immunix Secured OS Security Advisory, IMNX-2003-7+-012-01, June 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
FlashFXP [43]	Windows	FlashFXP 2.0, 2.0 build 905	Two vulnerabilities exist: a buffer overflow vulnerability exists when a server response to the PASV FTP command is handled, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists due to insufficient bounds of hostnames, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.flashfxp.com/download.php	FlashFXP Remote Buffer Overflows	**High**	Bug discussed in newsgroups and websites.
Frank Wallacher [44]	Windows, Unix	WebChat 2.0	Several vulnerabilities exist: a vulnerability exists in several PHP scripts when a malicious request is submitted, which could let a malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists in the 'users.php' script due to insufficient filtering of script code from URI parameters, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	WebChat Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Front Range Solutions [45]	Windows	GoldMine Business Contact Manager 6.00.30403, 6.00.30203, 6.00.21021, 5.70.30503, 5.70.20404	A vulnerability exists due to the way HTML e-mail is handled, which could let a remote malicious user execute arbitrary HTML and script code.	The vendor has patches available for GoldMine. Users are advised to contact the vendor at: http://support.frontrange.com/	GoldMine HTML E-Mail Script Execution CVE Name: CAN-2003-0241	**High**	Bug discussed in newsgroups and websites.
Gator Corporation[46]	Windows	eWallet 3.1	Several vulnerabilities exist: a vulnerability exists because private information is stored without encryption, which could let a malicious user obtain sensitive information; and a vulnerability exits because due to insufficient authentication of backups, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Gator EWallet Information Encoding Weakness	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[43] Bugtraq, June 9, 2003.
[44] Bugtraq, June 1, 2003.
[45] SECNAP Security Advisory, May 28, 2003.
[46] SecurityTracker Alert ID, 1006891, May 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GCC[47]	Unix	GNU gcc 3.2–7, 3.2, 3.2.1, 3.2.2-5, 3.2.2; RedHat gcc-3.2-7.i386.rpm, gcc-3.2.2-5.i386.rpm	A vulnerability exists in the GCC compiler, which could let a malicious user obtain sensitive information or execute arbitrary code.	Upgrade available at: http://gcc.gnu.org/releases.html	GNU GCC Compiler	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Geeklog[48]	Windows, Unix	Geeklog 1.3, 1.3.5 sr1&sr2, 1.3.5, 1.3.7 sr1, 1.3.7	Two vulnerabilities exist: a vulnerability exists due to insufficient sanitization of cookie values, which could let a remote malicious user execute arbitrary code; and a vulnerability exists due to insufficient validation of image upload extensions, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://www.geeklog.net/filemgmt/visit.php?lid=157	Geeklog Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Image upload extension vulnerability can be exploited via a web browser.
GNOME[49]	Multiple	Gnome 1.0.x, 1.1, 1.2	A remote Denial of Service vulnerability exists when processing NLST data due to a failure to sufficiently handle the size of returned data.	No workaround or patch available at time of publishing.	Gnome FTP NLST Data Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
GNU[50] ***Vendors issue advisories*** *[51, 52, 53, 54, 55]*	**Unix**	**GNU Privacy Guard 1.0-1.2.1**	**A vulnerability exists in the key validation code due to insufficient differentiation between the validity given to individual IDs on a public key that has multiple user IDs linked to it, which could let a malicious user obtain sensitive information.**	**Upgrade available at:** **http://www.gnupg.org/(en)/download/index.html#auto-ref-0** ***Engarde:*** **http://infocenter.guardiandigital.com/advisories/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***OpenPKG:*** **ftp.openpkg.org** ***RedHat:*** **ftp://updates.redhat.com/** ***Sun:*** **http://sunsolve.sun.com/patches/linux/security.html** ***YellowDog:*** **ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/**	**GNU Privacy Guard Insecure Trust Path To User ID** **CVE Name: CAN-2003-0255**	**Medium**	**Bug discussed in newsgroups and websites.**

[47] Bugtraq, May 28, 2003.
[48] SecurityTracker Alert ID: 1006879, May 29, 2003.
[49] Bugtraq, June 11, 2003.
[50] Bugtraq, May 4, 2003.
[51] Guardian Digital Security Advisory, ESA-20030515-016, May 15, 2003.
[52] OpenPKG Security Advisory, OpenPKG-SA-2003.029, May 16, 2003.
[53] Red Hat Security Advisory, RHSA-2003:175-01, May 21, 2003.
[54] Mandrake Linux Security Update Advisory, MDKSA-2003:061, May 22, 2003.
[55] Yellow Dog Linux Security Announcement, DU-20030602-4, June 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GNU[56]	Unix	man 1.5.1	A format string vulnerability exists when handling a catalog file, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Man Catalog File Format String	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Hanterm[57] ***RedHat issues patch***[58]	**Unix**	**hanterm-xf 2.0**	**A Denial of Service vulnerability exists because the terminal fails to sufficiently filter certain potentially malicious loop-based escape sequences.**	***RedHat:*** **ftp://updates.redhat.com/**	**Hanterm-XF Loop-Based Escape Sequence Denial of Service** **CVE Name: CAN-2003-0079**	**Low**	**Bug discussed in newsgroups and websites.**
Hanterm[59] ***RedHat issues patch***[60]	**Unix**	**hanterm-xf 2.0**	**A vulnerability exists in the window title reporting feature, which could let a malicious user execute arbitrary commands.**	***RedHat:*** **ftp://updates.redhat.com/**	**hanterm-xf Window Title Reporting Escape Sequence Command** **CVE Name: CAN-2003-0078**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Hewlett Packard Company[61]	Unix	HP-UX 10.20, 11.0, 11.11	A buffer overflow vulnerability exists in the UUCP and UUSUB implementations due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	Patches available at: ftp://hprc.external.hp.com/	HP-UX UUCP & UUSUB Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Hewlett Packard Company[62]	Unix	HP-UX ftpd 1.1.214 .4	A vulnerability exists in the 'REST' command when a specially calculated numeric argument is specified, which could let a remote malicious user obtain sensitive information.	Patch available at: http://itrc.hp.com PHNE_21936 patch release.	HP-UX FTPD REST Command	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Hewlett Packard Company[63]	Unix	HP-UX 10.20	A buffer overflow vulnerability exists in the 'pcltotiff' program due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	HPUX PCLToTIFF Command Line Argument Local Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[56] Bugtraq, June 3, 2003.
[57] Bugtraq, February 24, 2003.
[58] Red Hat Security Advisory, RHSA-2003:070-01, June 6, 2003.
[59] Bugtraq, February 24, 2003.
[60] Red Hat Security Advisory, RHSA-2003:070-01, June 6, 2003.
[61] Hewlett-Packard Company Security Bulletin, HPSBUX0306-262, June 2, 2003.
[62] Secure Network Operations, Inc. Advisory, SRT2003-06-05-0935, June 5, 2003.
[63] Bugtraq, June 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company[64] ***Proof of Concept exploit published***[65]	**Unix**	**HP-UX 10.0 1, 10.0, 10.1, 10.8-10.10, 10.16, 10.20, 10.24, 10.26, 10.30, 10.34, 11.04, 11.0, 11.11, 11.20, 11.22**	**A vulnerability exists in the 'rs.F3000' binary, which could let a malicious user obtain unauthorized access or cause a Denial of Service.**	**Workaround:** **Remove the execute permissions on the affected binary by issuing the following commands:** **chmod 444 /usr/lib/X11/Xserver/ucode/screens/hp/rs.F3000**	**HP-UX rs.F3000 Unauthorized Access**	**Low/ Medium** **(Medium if access can be obtained)**	**Bug discussed in newsgroups and websites.** ***Proof of Concept exploit has been published.***
Hewlett Packard Company[66] ***Another exploit script published***[67]	**Unix**	**HP-UX 10.0 1, 10.0, 10.1, 10.8-10.10, 10.16, 10.20, 10.24, 10.26, 10.30, 10.34, 11.04, 11.0, 11.11, 11.20, 11.22**	**A buffer overflow vulnerability exists in the 'stmkfont' utility, which could let a malicious user obtain elevated privileges.**	**Patches available at:** **http://itrc.hp.com/** **Patch PHSS_15423** **Workaround:** **For HP-UX 11 systems, it is advised to remove the setuid bit of stmkfont by issuing the following command:** **chmod 555 /usr/bin/stmkfont**	**HP-UX 'stmkfont' Buffer Overflow**	**Medium**	**Bug discussed in newsgroups and websites. Exploit has been published.**
Hewlett Packard Company[68]	Unix	HP-UX 11.0, 11.11, 11.22	A Denial of Service vulnerability exists due to the way certain network traffic is handled.	Patches available at: http://itrc.hp.com	HP-UX Network Traffic Denial of Service	Low	Bug discussed in newsgroups and websites.
IBM[69]	Unix	AIX 4.3-4.3.3, 5.1	A buffer overflow vulnerability exists in the 'lsmcode' utility due to insufficient bounds checking, which could let a malicious user execute arbitrary instructions with elevated privileges.	No workaround or patch available at time of publishing.	AIX 'LSMCODE' Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
interMute, Inc.[70]	Windows	AdSubtract Proxy 2.50-2.55	A vulnerability exists in the banner ad blocking software due to a failure to handle specially crafted hostnames when carrying out reverse DNS lookups, which could let a remote malicious user bypass the access control list.	No workaround or patch available at time of publishing.	AdSubtract Bypass Connection Proxying	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[64] Hewlett-Packard Company Security Bulletin, HPSBUX0302-240, February 12, 2003.
[65] SecurityFocus, June 9, 2003.
[66] Hewlett-Packard Company Security Bulletin, HPSBUX0302-241, February 12, 2003.
[67] SecurityFocus, June 9, 2003.
[68] Hewlett-Packard Company Security Bulletin, HPSBUX0306-264, June 4, 2003.
[69] Securiteam, June 11, 2003.
[70] SecurityTracker Alert ID, 1006925, June 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
John Roy[71]	Multiple	Pi3Web 2.0.2 Beta1	A buffer overflow vulnerability exists in the 'Name' column of the Directory Index due to insufficient bounds checking, which could let a remote malicious user cause a Denial of Service or possibly execute arbitrary code.	Upgrade available at: http://osdn.dl.sourceforge.net/sourceforge/pi3web/Pi3Web-x86Win32-2_0_2-beta2.exe	Pi3Web Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
KDE[72, 73, 74] ***More updates issued***[75, 76, 77, 78] ***RedHat releases update***[79] ***Sun issues patches***[80]	**Unix**	**KDE 2.0-3.1.1**	**A vulnerability exists when specially formatted PDF and PS files are processed due to the way the Ghostscript software is used, which could let a malicious user execute arbitrary commands.**	**KDE:** **http://download.kde.org/stable/3.0.5b/** **Debian:** **http://security.debian.org/pool/updates/main/k/kdegraphics/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***SuSE:*** **ftp://ftp.suse.com/pub/suse** ***Debian:*** **http://security.debian.org/pool/updates/main/k/kdelibs/** **http://security.debian.org/pool/updates/main/k/kdebase/kde** ***RedHat:*** **ftp://updates.redhat.com/** ***Sun:*** **http://sunsolve.sun.com/patches/linux/security.html**	**KDE Postscript/ PDF File Processing** **CVE Name: CAN-2003-0204**	**High**	**Bug discussed in newsgroups and websites.**
KDE[81] ***Upgrades now available***[82, 83]	**Unix**	**Konqueror Embedded 0.1**	**A vulnerability exists because the Common Name (CN) field on X.509 certificates is not properly validated when a SSL/TLS session is negotiated, which could let a malicious server masquerade as a trusted server.**	***KDE:*** **ftp://ftp.kde.org/pub/kde/security_patches** ***RedHat:*** **ftp://updates.redhat.com/**	**Konqueror Embedded Common Name Certificate Validation**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**

[71] Tripbit Advisory TA-2003-05, June 2, 2003.
[72] KDE Security Advisory, April 9, 2003.
[73] Debian Security Advisory, DSA 284-1, April 12, 2003.
[74] Sorcerer Update Advisory SORCERER2003-04-12, April 12, 2003.
[75] Mandrake Linux Security Update Advisory, MDKSA-2003:049, April 17, 2003.
[76] SuSE Security Announcement, SuSE-SA:2003:0026, April 24, 2003.
[77] Debian Security Advisory, DSA 293-1, April 23, 2003.
[78] Debian Security Advisory, DSA 296-1, April 30, 2003.
[79] Red Hat Security Advisory, RHSA-2003:002-01, May 12, 2003.
[80] SecurityFocus, June 2, 2003.
[81] Bugtraq, May 7, 2003.
[82] KDE Security Advisory, June 2, 2003.
[83] Red Hat Security Advisory, RHSA-2003:192-01, June 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
LeapWare[84]	Windows	LeapFTP 2.7.3 .600	A buffer overflow vulnerability exists when a server response to the PASV FTP command is handled, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.leapware.com/download.html	LeapFTP PASV Command Response Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
lv[85, 86] ***Yellow Dog issues patch[87]***	**Unix**	**lv 4.49.1-4.49.4; RedHat lv-4.49.4-1.i386.rpm, lv-4.49.4-3.i386.rpm , lv-4.49.4-7.i386.rpm , lv-4.49.4-9.i386.rpm**	**A vulnerability exists in the lv multilingual file viewer, which could let a malicious user execute arbitrary commands.**	**Upgrade available at:** **http://www.ff.iij4u.or.jp/~nrt/freeware/lv4495.tar.gz** **Debian:** **http://security.debian.org/pool/updates/main/l/lv/** **RedHat:** **ftp://updates.redhat.com/** ***YellowDog:*** **ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/**	**lv Configuration File** **CVE Name: CAN-2003-0188**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Max Yuan[88]	Windows	MaxWeb Portal 1.30	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'search.asp' script, which could let a remote malicious user execute arbitrary script code; a vulnerability exists because the 'start new topic' page may be modified off-line, which could let a remote malicious user corrupt certain field values; a vulnerability exists because a session cookie can be retrieved, which could let a remote malicious user hijack a user's account; an information disclosure vulnerability exists because database files are not secured properly, which could let a remote malicious user obtain sensitive information; and a vulnerability exits in the 'password.asp' script because a forgotten password may be reset off-line, which could let a remote malicious user obtain unauthorized access.	Patch available at: http://www.gulftech.org/vuln/MaxWebPortal%201.30%20Patch.zip	Multiple MaxWebPortal Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[84] Bugtraq, June 9, 2003.
[85] Debian Security Advisory, DSA 304-1, May 15, 2003.
[86] Red Hat Security Advisory, RHSA-2003:169-01, May 16, 2003.
[87] Yellow Dog Linux Security Announcement, YDU-20030602-6, June 2, 2003.
[88] SecurityTracker Alert ID, 1006944, June 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Michel Valdrighi[89]	Windows, Unix	Cafelog b2 0.6 pre, pre2, 0.6.1	A vulnerability exists in the 'blogger-2-b2.php' and 'gm-2-b2.php' scripts due to insufficient sanitization of user-supplied variables, which could let a remote malicious user execute arbitrary code and obtain administrative privileges.	No workaround or patch available at time of publishing.	Cafelog b2 Remote File Include	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Michel Valdrighi[90]	Windows, Unix	Cafelog b2 0.6.1	A vulnerability exists in the 'b2functions.php' script due to insufficient sanitization of user-supplied values, which could let a remote malicious user execute arbitrary instructions	No workaround or patch available at time of publishing.	Cafelog b2 'B2Functions' Script	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Michel Valdrighi[91]	Windows, Unix	Cafelog b2 0.6 pre2, 0.6 pre, 0.6.1, 0.6.2	Several vulnerabilities exist: a vulnerability exists in the 'blog.header.php' script due to insufficient sanitization of user-supplied input, which could let a malicious user execute arbitrary code; and a vulnerability exists in the 'B2MenuTop' script due to insufficient sanitization of user-supplied values, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	b2 'Blog.Header' & 'B2MenuTop' Scripts	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[92]	Windows 2003	Windows Server 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition , 64-bit, 2003 Standard Edition , 2003 Web Edition	A vulnerability exists because several NIC (Network Interface Card) device drivers pad frames with content from previous packets or kernel memory instead of using NULL-bytes during a FIN-ACK exchange when closing a TCP connection, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Microsoft Windows NIC Information Disclosure	Medium	Bug discussed in newsgroups and websites.

[89] Secunia Security Advisory, May 30, 2003.
[90] SecurityFocus, June 2, 2003.
[91] SecurityTracker Alert, 1006933, June 6, 2003.
[92] NGSSoftware Insight Security Research Advisory, June 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[93]	Windows XP	XP 64-bit Edition, SP1, XP Embedded, SP1, XP Home, SP1, XP Media Center Edition , XP Professional, SP1, XP Tablet PC Edition	A Denial of Service vulnerability exists due to a failure to handle certain conditions involving multiple nested directories.	No workaround or patch available at time of publishing.	Windows XP Nested Directory Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[94]	Windows 95/98/ME/ NT 4.0/2000/ 2003	Internet Explorer 5.0.1, SP1-SP3, 5.5, SP1&SP2, 6.0, SP1	Several vulnerabilities exist: a buffer overflow vulnerability exists because an object type returned from a web server is not properly identified, which could let a malicious user execute arbitrary code; and a vulnerability exists because an appropriate block on a file download dialog box is not implemented, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-020.asp	Microsoft Internet Explorer OBJECT Tag Buffer Overflow CVE Names: CAN-2003-0309, CAN-2003-0344	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[95]	Windows 95/98/ME/ NT 4.0/2000/ 2003	Internet Explorer 5.0.1, SP1-SP3, 5.5, SP1&SP2, 6.0, SP1	A vulnerability exists in the FTP indexing implementation when IE FTP is used in 'Classic Mode,' which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Internet Explorer Classic Mode FTP Client	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft[96]	Windows 98/ME/NT 4.0/2000/ 2003	Internet Explorer 6.0, SP1,	A vulnerability exists in the address of a "Cannot find server" page, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Internet Explorer %USER-PROFILE% File Execution	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[93] SecurityFocus, June 2, 2003.
[94] Microsoft Security Bulletin MS03-020 V1.1, June 4, 2003.
[95] SecurityFocus, June 4, 2003.
[96] Bugtraq, June 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [97]	Windows 2000/XP/ 2003	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Workstation, SP1-SP3, Windows Server 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, XP 64-bit Edition Version 2003, XP Embedded, SP1, XP Media Center Edition, XP Home, SP1, XP Professional, SP1, XP Tablet PC Edition	A remote Denial of Service vulnerability exists when IPV6 is enabled on the target server and a malicious user launches an ICMP flood attack.	No workaround or patch available at time of publishing.	Windows 2000/XP/2003 IPV6 Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Mini HTTP Server[98]	Windows 2000, XP	Forum Web Server 1.6	A vulnerability exists because authentication credentials are stored in plaintext, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Forum Web Server Insecure Authentication Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[97] SecurityFocus, June 2, 2003.

[98] Securiteam, May 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mirabilis [99]	Windows	ICQ Lite Build 1150	A vulnerability exists due to insecure folder permissions, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ICQ Lite Insecure Folder Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
mnoGo Search[100]	Windows, Unix	mnoGo Search 3.2.10, 3.1.20	Two buffer overflow vulnerabilities exist due to boundary errors when handling user input supplied to the 'ul' and 'tmplt' parameters, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.mnogosearch.org/download.html	MNOGoSearch 'ul' & 'tmplt' Parameters Buffer Overflows	**High**	Bug discussed in newsgroups and websites. Proofs of Concept exploit scripts have been published.
Monkey [101]	Unix	Monkey HTTP Daemon 0.1.4, 0.4-0.4.2, 0.5, 0.5.1, 0.6-0.6.3, 0.7 .0, 0.7.1	Several vulnerabilities exist: Cross-Site Scripting vulnerabilities exist in the '/php/index.php' and 'cgi-bin/test.pl' scripts, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in the 'test.pl' script due to insufficient HTML filtering, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	HTTP Cross-Site Scripting	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
M-Tech Information Technology [102]	Windows NT 4.0/2000	P-Synch 6.2.5	Multiple vulnerabilities exist: a vulnerability exists when an empty URL parameter is passed, which could let a malicious user obtain sensitive information; a Cross-Site Scripting vulnerability exists due to insufficient filtering of HTML code from URI parameters, which could let a remote malicious user execute arbitrary code; and a vulnerability exists due to insufficient sanitization of some user-supplied URI variables, which could let a remote malicious user execute arbitrary code.	Customers are advised to contact the vendor for fixes.	M-TECH P-Synch Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.

[99] SecurityFocus, June 5, 2003.
[100] Securiteam, June 11, 2003.
[101] Secunia Security Advisory, June 6, 2003.
[102] Bugtraq, May 29, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts

Multiple Vendors [103]	Windows 95/98/ME/ NT 4.0/2000, XP, 2003
	Unix
		Mozilla Browser 1.0, RC1&RC2, 1.0.1, 1.1-1.2.1, 1.3, 1.3.1;
		Netscape Communicator 7.0-7.02, 4.0, 4.5-4.79;
		Opera Software Opera Web Browser 6.0, Win32, 6.0.1, Win32, Linux, 6.0.2-6.0.5 Win32, Linux, 7.0-7.0.3 Win32, 7.10, 7.11
			A vulnerability exists because it is possible to violate the cross-domain browser security restriction, which could let a remote malicious user bypass security restrictions and execute arbitrary code.	No workaround or patch available at time of publishing.	Multiple Browser Cross-Platform	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

Multiple Vendors [104, 105]	Unix	kon2 kon2 0.3.9b; RedHat kon2-0.3.9b-13.i386. rpm, kon2-0.3.9b-16.i386. rpm, kon2-0.3.9b-6.i386.rpm, kon2-0.3.9b-7.i386.rpm	A buffer overflow vulnerability exists in the command line parsing code portion of the kon program due to insufficient bounds checking, which could let a malicious user obtain root privileges.	**Mandrake:** http://www.mandrakesecure.net/en/ftp.php **RedHat:** ftp://updates.redhat.com/	Multiple Vendor kon2 Buffer Overflow CVE Name: CAN-2002-1155	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors [106, 107]	Unix	GNU gzip 1.2.4 a, 1.2.4, 1.3, 1.3.2, 1.3.3, 1.3.5	A vulnerability exists in the 'znew' script due to a failure to securely handle temporary files, which could let a malicious user obtain elevated privileges.	**OpenPKG:** ftp://ftp.openpkg.org/release/1.1/UPD/ **Debian:** http://security.debian.org/pool/updates/main/g/gzip/	GZip ZNew Insecure Temporary File Creation CVE Name: CAN-2003-0367	Medium	Bug discussed in newsgroups and websites.

[103] Bugtraq, June 7, 2003.
[104] Red Hat Security Advisory, RHSA-2003:047-01, June 3, 2003.
[105] Mandrake Linux Security Update Advisory, MDKSA-2003:064, June 5, 2003.
[106] Debian Security Advisory, DSA 308-1, June 7, 2003.
[107] OpenPKG Security Advisory, OpenPKG-SA-2003.031, June 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[108]	Unix	GNU gzip 1.2.4a, 1.2.4, 1.3, 1.3.2	A vulnerability exists in 'gzexe' because temporary files are used insecurely, which could let a malicious user obtain elevated privileges.	**Debian:** http://security.debian.org/pool/updates/main/g/gzip/	GNU gzexe Escalated Privileges	Medium	Bug discussed in newsgroups and websites.

Multiple Vendors[109]
Patch now available[110]
	Unix	**HP HP-UX 10.20, 10.24, 10.26, 10.30, 10.34, 11.04, 11.0, 11.11, 11.20, 11.22;**
		IBM AIX 4.3-4.3.3, 5.1, 5.2;
		SGI IRIX 5.0, 5.0.1, 5.1, 5.1.1, 5.2, 5.3, 6.0, 6.0.1, 6.1-6.5.19, 6.5.2 m-6.5.18 m, 6.5.2 f-6.5.18 f;
		Sun Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86
			A vulnerability exists in dtterm's window title reporting feature, which could let a malicious user execute arbitrary commands.	***Patch available at:***
				ftp://ftp.itrc.hp.com/export/patches/hp-ux_patch_matrix/
					DTTerm Window Title Reporting Escape Sequence Command
					CVE Name: CAN-2003-0064
						High	**Bug discussed in newsgroups and websites. There is no exploit code required.**

[108] Debian Security Advisory, DSA 308-1, June 6, 2003.
[109] Bugtraq, February 24, 2003.
[110] Hewlett-Packard Company Security Bulletin, HPSBUX0306-263, June 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [111, 112] ***Yellow Dog issues advisory*** [113]	**Unix**	**Apache Software Foundation Apache 2.0.37-2.0.45; RedHat httpd-2.0.40-21.i386.rpm, 40-8.i386.rpm, httpd-devel-2.0.40-21.i386.rpm, 2.0.40-8.i386.rpm, httpd-manual-2.0.40-21.i386.rpm, 2.0.40-8.i386.rpm, mod_ssl-2.0.40-21.i386.rpm, 2.0.40-8.i386.rpm**	**A vulnerability exists in the 'apr_password_validate()' function due to improper use of specific thread-safe functions, which could let a remote malicious user cause a Denial of Service.**	**Apache:** **http://www.apache.org/dist/httpd/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **RedHat:** **ftp://updates.redhat.com/** ***YellowDog:*** **ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/**	**Apache Basic Authentication Module Denial of Service** **CVE Name: CAN-2003-0189**	**Low**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**
Multiple Vendors [114, 115,]	Unix	Linux kernel 2.4.0-test1-test12, 2.4-2.4.20	A remote Denial of Service vulnerability exists because some types of network traffic are not properly handled.	**Debian:** http://security.debian.org/pool/updates/main/k/ **RedHat:** ftp://updates.redhat.com/	Linux Kernel Excessive Traffic Remote Denial of Service CVE Name: CAN-2003-0364	Low	Bug discussed in newsgroups and websites.

[111] Red Hat Security Advisory, RHSA-2003:186-01, May 28, 2003.
[112] iDEFENSE Security Advisory, May 30, 2003.
[113] Yellow Dog Linux Security Announcement, YDU-20030603-1, June 3, 2003.
[114] Red Hat Security Advisory, RHSA-2003:187-01, June 3, 2003.
[115] Debian Security Advisories, DSA 311-1 & 312-1, June 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [116, 117, 118]	Unix	Linux kernel 2.0-2.0.39, 2.1, 2.1.89, 2.2-2.2.25, 2.3, 2.3.99, 2.3.99 pre1-pre7, 2.3.99, 2.4.0-test1-test12, 2.4-2.4.21 pre4, 2.5.0-2.5.69; RedHat Linux 7.1, i386, i586, i686, 7.2, athlon, i386, i586, i686, 7.3, i386, i686, 8.0, i386, i686, 9.0 i386	A Denial of Service vulnerability exists in the TTY layer.	**Debian:** http://security.debian.org/pool/updates/main/k/ **Mandrake:** ftp://ftp.planetmirror.com/pub/Mandrake/updates/9.1/RPMS/ **RedHat:** ftp://updates.redhat.com/	Linux TTY Layer Denial of Service CVE Name: CAN-2003-0247	Low	Bug discussed in newsgroups and websites.
Multiple Vendors [119, 120, 121]	Unix	Linux kernel 2.4.0-test1-test12, 2.4-2.4.20, 2.4.21 pre1&pre4	A vulnerability exists in the MXCSR handler code due to a failure to handle malformed address data.	**Debian:** http://security.debian.org/pool/updates/main/k/ **Mandrake:** ftp://ftp.planetmirror.com/pub/Mandrake/updates/9.1/RPMS/ **RedHat:** ftp://updates.redhat.com/	Linux Kernel MXCSR Handler Malformed Address CVE Name: CAN-2003-0248	Low	Bug discussed in newsgroups and websites.

[116] Red Hat Security Advisory, RHSA-2003:187-01, June 3, 2003.
[117] Debian Security Advisories, DSA 311-1 & 312-1, June 9, 2003.
[118] Mandrake Linux Security Update Advisory, MDKSA-2003:066, June 11, 2003.
[119] Red Hat Security Advisory, RHSA-2003:187-01, June 3, 2003.
[120] Debian Security Advisories, DSA 311-1 & 312-1, June 9, 2003.
[121] Mandrake Linux Security Update Advisory, MDKSA-2003:066, June 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [122, 123, 124, 125] ***More vendors release advisories*** [126, 127]	**Unix**	**EnGarde Guardian Digital WebTool 1.2; Webmin Usermin 0.4- 0.99, 1.0 50, 1.0 60**	**A vulnerability exists in the 'Miniserv.pl' script due to insufficient sanitization of client-supplied BASE64 encoded input, which could let a malicious user bypass authentication procedures and obtain administrative access.**	**EnGarde:** **http://ftp.engardelinux.org/pub/engarde/stable/updates/noarch/** **Webmin:** **http://www.webmin.com/udownload.html** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** ***Debian:*** **http://security.debian.org/pool/updates/main/w/webmin/** ***SGI:*** **ftp://patches.sgi.com/support/free/security/patches/6.5.20/**	**Webmin/ Usermin 'Miniserv.pl' Authentication Bypass** **CVE Name: CAN-2003-0101**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
myServer [128]	Windows, Unix	myServer 0.4.1	A buffer overflow vulnerability exists when processing HTTP GET requests that are of excessive length, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	myServer Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
newsPHP [129]	Windows, Unix	newsPHP	A vulnerability exists in the 'comments' feature due to insufficient sanitization of HTML, which could let a remote malicious user execute arbitrary HTML and script code.	Users are advised to contact the vendor for further details.	newsPHP Comment Feature HTML Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Nokia[130]	Multiple	GGSN (IP650 based) Release 1	A remote Denial of Service vulnerability exists in GGSN devices when a specifically malformed IP packet is submitted.	Affected users running vulnerable systems should contact Nokia for fix information.	GGSN Remote Denial of Service CVE Name: CAN-2003-0368	Low	Bug discussed in newsgroups and websites.
Novell[131]	Multiple	iChain Server 2.2, FP1	A vulnerability exists in the 'NCPIP.NLM' and 'JSTCP.NLM' resources due to inadequate authentication, which could let a remote malicious user obtain unauthorized access to restricted resources.	Patches available at: http://support.novell.com/servlet/filedownload/ftf/	iChain Inadequate Authentication	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[122] Gentoo Linux Security Announcement, 200302-12, February 22, 2003.
[123] Gentoo Linux Security Announcement, 200302-14, February 24, 2003.
[124] EnGarde Secure Linux Security Advisory, ESA-20030225-006, February 25, 2003.
[125] Mandrake Linux Security Update Advisory, MDKSA-2003:025, February 26, 2003.
[126] SGI Security Advisory, 20030602-01-I, June 9, 2003.
[127] Debian Security Advisory, DSA 319-1, June 12, 2003.
[128] SecurityFocus, June 2, 2003.
[129] Exploitlabs.com Advisory 003, EXPL-A-2003-003, June 5, 2003.
[130] @stake Inc. Security Advisory, June 9, 2003.
[131] Novel Security Alert, NOVL-2003-2966205, June 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Novell[132]	Multiple	iChain Server 2.1, SP1&SP2, 2.2, FP1	A buffer overflow vulnerability exists in the username supplied during authentication due to insufficient bounds checking, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	Patches available at: http://support.novell.com/servlet/filedownload/ftf/	iChain Server Remote Authentication Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
Novell[133]	Multiple	Netware 6.0, SP1&SP2	A remote Denial of Service vulnerability exists because malformed packets are not handled properly.	Patches available at: http://support.novell.com/servlet/filedownload/ftf/httpstk3.exe/	Netware HTTP Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
nPHP[134]	Multiple	nPHP 216	A vulnerability exists in the 'e-mail' field due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	NPHP Remote Privilege Escalation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Nuca[135]	Multiple	Nuca WebServer 0.1	A Directory Traversal vulnerability exists due to an input validation error, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Nuca WebServer Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
OpenSSH[136]	MacOS X 10.x, Unix	OpenSSH 3.0, p1, 3.0.1, p1, 3.0.2, p1, 3.1, p1, 3.2, 3.2.2 p1, 3.2.3 p1, 3.3, p1, 3.4, p1, 3.5, 3.6.1, p1&p2	A vulnerability exists in the way access is restricted, which could let an unauthorized remote malicious user bypass host access restrictions.	No workaround or patch available at time of publishing.	OpenSSH Access Control Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[132] Novel Security Alerts, NOVL-2003-2966205 & NOVL-2003-2966207, June 5, 2003.
[133] Novell Security Alert, NOVL-2003-2966181, June 6, 2003.
[134] SecurityFocus, June 5, 2003.
[135] Secunia Security Advisory, June 11, 2003.
[136] Welkyn Security Advisory, SA-2003060400, June 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Pablo Software Solutions [137]	Windows	Baby FTP Server 1.2	Two vulnerabilities exist: a Directory Traversal vulnerability exists due to an input validation error in the 'CWD' command, which could let a remote malicious user obtain sensitive information; and a remote Denial of Service vulnerability exists when multiple connections are established from the same IP address.	No workaround or patch available at time of publishing.	Baby FTP Server Directory Traversal	Low/ Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.
Pablo Software Solutions [138]	Windows	FTP Server 1.2	Several vulnerabilities exist: a vulnerability exists due to insufficient restrictions of the anonymous user account, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in the 'users.dat' file because passwords are stored in plaintext, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	FTP Server Anonymous Users & Plaintext Password Storage	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Phil Ward[139]	Windows	philboard 1.14	Two vulnerabilities exist: a vulnerability exists in the 'philboard_admin.asp' script during authentication, which could let a remote malicious user obtain administrative access; and a vulnerability exists because the 'philboard.mdb' database is publicly accessible, which could let a remote malicious user retrieve the database.	No workaround or patch available at time of publishing.	Philboard Administrative Access & Database Access	Medium/ **High** **(High if administrative access can be obtained)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
PHP[140]	MacOS X 10.x, Unix	PHP 4.0-4.0.7, 4.1.0-4.1.2, 4.2.0-4.2.3, 4.3, 4.3.1	A Cross-Site Scripting vulnerability exists in the phpinfo() debugging function, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	PHP PHPInfo Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[137] Secunia Security Advisory, June 2, 2003.
[138] Bugtraq, June 3, 2003.
[139] Bugtraq, May 29, 2003.
[140] Bugtraq, June 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PoPToP [141] ***Debian issues advisory*** [142] ***SuSE issues advisory*** [143]	**Unix**	**PPTP Server 1.0.1, 1.1.2-1.1.4-b2**	**A buffer overflow vulnerability exists due to insufficient sanity checks when referencing user-supplied input used in various calculations, which could let a remote malicious user execute arbitrary code**	**Upgrade available at:** **http://sourceforge.net/project/showfiles.php?group_id=44827** ***Debian:*** **http://security.debian.org/pool/updates/main/p/pptpd** ***SuSE:*** **ftp://ftp.suse.com/pub/suse**	**PoPToP PPTP Remote Buffer Overflow** **CVE Name: CAN-2003-0213**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***
Positive Software [144]	Unix	H-Sphere 2.0 6, 2.0 5, 2.0, 2.1-2.3 RC3	Several Cross-Site Scripting vulnerabilities exists in the 'template_name' and 'ftemplate' parameters due to insufficient filtering of HTML and script code, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	H-Sphere HTML Template Inclusion Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Quality On Line Ltd. [145]	Windows	IRCXpro Server 1.0	A vulnerability exists in the 'settings.ini' file due to the method used for password storage, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	IRCXpro Server 'Settings.INI' Password Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Quality Programming Corporation[146]	Windows	Mega-Browser 0.3	Multiple vulnerabilities exist: a Directory Traversal vulnerability exists in the HTTP directory, which could let a remote malicious user obtain sensitive information; and a vulnerability exists when attempting to authenticate via the FTP service due to a user enumeration weakness, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	MegaBrowser Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Directory Traversal vulnerability can be exploited via a web browser. There is no exploit code required for the FTP server vulnerability.

[141] Bugtraq, April 9, 2003.
[142] Debian Security Advisory, DSA 295-1, April 30, 2003.
[143] SuSE Security Announcement, SuSE-SA:2003:029, June 6, 2003.
[144] SecurityTracker Alert ID, 1006961, June 9, 2003.
[145] Exploitlabs.com Advisory 002, June 3, 2003.
[146] Bugtraq, June 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
RedHat[147] *Sun issues patched*[148]	**Unix**	**Linux 7.1, 7.1 k i386, ia64, i386, alpha, 7.2, 7.2 ia64, i386, alpha, 7.3 i386, 8.0 i386, 9.0 i386, tcpdump-3.4 - 39.i386.rpm, tcpdump-3.6.2-12.i386.rpm, tcpdump-3.6.2-9.i386.rpm, tcpdump-3.6.2-9.ia64.rpm, tcpdump-3.6.3-3.i386.rpm, tcpdump-3.7.2-.i386.rpm**	**A vulnerability exists due to a compilation error design in tcpdump, which would let tcpdump continue running as "root" rather than the less privileged user "pcap."** ***Note: This is not a vulnerability in itself, since it could only be exploited if another vulnerability is present.***	**Upgrade available at: ftp://updates.redhat.com/** ***Sun:*** **http://sunsolve.sun.com/patches/linux/security.html**	**Red Hat Linux tcpdump Privilege Retention** **CVE Name: CAN-2003-0194**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
RedHat[149]	Unix	RedHat Linux 7.1, i386, i586, i686, 7.2, athlon, i386, i586, i686, 7.3, i386, i686, 8.0, i386, i686, 9.0 i386	A vulnerability exists under very restrictive circumstances because a file may be simultaneously unlinked and the corresponding mapped file blocks reallocated, which could let a malicious user corrupt arbitrary files.	Upgrade available at: ftp://updates.redhat.com/	Red Hat Linux EXT3 Filesystem Data Corruption	Medium	Bug discussed in newsgroups and websites.
RhinoSoft[150]	Windows	FTP Voyager 9.1 .0.3, 10.0 .0.0	A buffer overflow vulnerability exists because long filenames are handled incorrectly when they are returned in response to a "LIST" request, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.ftpvoyager.com/	FTP Voyager Remote LIST Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[147] Red Hat Security Advisory, RHSA-2003:174-01, May 15, 2003.
[148] SecurityFocus, June 9, 2003.
[149] Red Hat Security Advisory, RHSA-2003:187-01, June 3, 2003.
[150] Bugtraq, June 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
RPM[151]	Multiple	RPM Package Manager 4.1	A remote Denial of Service vulnerability exists when processing NLST data due to a failure to sufficiently handle the size of returned data.	No workaround or patch available at time of publishing.	RPM Package Manager FTP NLST Data Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Russell Marks[152]	Unix	zblast 1.2	A buffer overflow vulnerability exists in the 'ZBLAST_NAME,' 'USER,' and 'LOGNAME' variables when data is copied, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Zblast Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
SaarPort. net[153]	Windows, Unix	SPChat 0.8	A Cross-Site Scripting vulnerability exists in the 'statussess' variable due to insufficient sanitization, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	SPChat Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
SGI[154]	Unix	IRIX 6.5-6.5.20, 6.5.2f-6.5.20f, 6.5.2m-6.5.20m	A Denial of Service vulnerability exists because the 'PIOCSWATCH' option is not properly handled.	Patches available at: ftp://patches.sgi.com/support/free/security/patches/	IRIX 'PIOCS-WATCH' Denial of Service CVE Name: CAN-2003-0175	Low	Bug discussed in newsgroups and websites.
SmartFTP[155]	Windows	SmartFTP 1.0.973	Two vulnerabilities exist: a buffer overflow vulnerability exists when a 'PWD' command is submitted to an FTP server, which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability exists when a File List command is issued to an FTP server, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.smartftp.com/download/	SmartFTP Remote Buffer Overflows	**High**	Bug discussed in newsgroups and websites.
SMC Networks[156]	Multiple	SMC 7004VWBR 1.22	A remote Denial of Service vulnerability exists due to an error in the way certain packets are handled.	Upgrade available at: http://www.smc.com/drivers_downloads/library/7004VWBR_FWv123.zip	SMC Wireless Router Packet Remote Denial of Service CVE Name: CAN-2003-0419	Low	Bug discussed in newsgroups and websites.

[151] Bugtraq, June 11, 2003.
[152] Bugtraq, June 5, 2003.
[153] Bugtraq, May 31, 2003.
[154] SGI Security Advisory, 20030603-01-P, June 10, 2003.
[155] NTBugtraq, June 9, 2003.
[156] iDEFENSE Security Advisory, June 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Soft Activity. com[157]	Windows	Activity Monitor 2002 2.6	A remote Denial of Service vulnerability exists when a malicious user submits large packets to port 15163/tcp.	No workaround or patch available at time of publishing.	Activity Monitor 2002 Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Speak Freely[158]	Windows, Unix	Speak Freely 7.1 Speak Freely 7.5	Several vulnerabilities exist: a buffer overflow vulnerability exists due to the way UDP packets are handled with the "faceRequest" bit set, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists due to the way VAT protocol packets are handled, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists when audio packets are decompressed, which could let a remote malicious user execute arbitrary code; a race condition vulnerability exists when PGP is used, which could let a malicious user overwrite arbitrary files; and a vulnerability exists because a function allows UDP packets to be echoed back to the sender, which could let a malicious user relay arbitrary packets.	No workaround or patch available at time of publishing.	Multiple Speak Freely Remote Boundary Condition Error Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Spyke-Online[159]	Multiple	Spyke PHP Board 2.1	Multiple vulnerabilities exist because the CMS uses plaintext files for storage of configuration data, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Spyke PHP Board Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Squirrel Mail[160] ***Yellow Dog issues update[161]***	**Unix**	**Squirrel-Mail 1.0.4, 1.0.5, 1.2.0-1.2.10**	**Multiple Cross-Site Scripting vulnerabilities exist, which could let a malicious user execute arbitrary HTML and script code.**	**SquirrelMail:** **http://www.squirrelmail.org/download.php** **RedHat:** **ftp://updates.redhat.com/** ***YellowDog:*** **ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/**	**Multiple SquirrelMail Cross-Site Scripting** **CVE Name: CAN-2003-0160**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required.**

[157] Securiteam, May 30, 2003.
[158] Secunia Security Advisory, June 10, 2003.
[159] theblacksheep&erik Advisory, June 9, 2003.
[160] Red Hat Security Advisory, RHSA-2003:112-01, April 24, 2003.
[161] Yellow Dog Linux Security Announcement, YDU-20030602-2, June 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[162]	Windows, Unix	SDK & JRE (Windows Production Release) 1.3.1_02 & prior, 1.3.0_05 & prior, 1.2.2_010 & prior, JDK 1.1.8_008 & prior, (Solaris OE Reference Releases) SDK & JRE 1.2.2_010 & prior, JDK 1.1.8_008 & prior, Solaris OE Production Releases SDK & JRE 1.3.1_02 & prior, 1.3.0_05 & prior, 1.2.2_10 & prior, JDK 1.1.8_14 & prior, (Linux Production Release) SDK & JRE 1.3.1_02 & prior, 1.3.0_05 & prior, 1.2.2_010 & prior	Several vulnerabilities exist: a vulnerability exists in the Java Runtime Environment (JRE) due to insufficient resource restriction, which could let a malicious user obtain unauthorized access to restricted resources; a vulnerability exists in the Java Runtime Environment (JRE). because it is possible for an untrusted Java applet to gain access to properties of HTTP requests, which could let a malicious user obtain sensitive information; and a vulnerability exists in the Sun Java Runtime Environment through the use of a malicious Java Plugin, which could let a malicious user obtain unauthorized access.	Upgrades available at: http://java.sun.com/j2se/	JRE Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites.

[162] Sun(sm) Alert Notification, 55101, June 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[163]	Windows, Unix	SDK & JRE (Windows Production Release) 1.4.0_01 & prior, 1.3.1_04 & prior, 1.3.0_05 & prior, 1.2.2_012 & prior, SDK & JRE (Solaris Production Release)0 1.4.0_01 & prior, 1.3.1_04 & prior, 1.3.0_05 & prior, 1.2.2_12 & prior, Solaris Operating Environ-ment (OE) Reference Releases 1.2.2_012 & prior, SDK & JRE (Linux Production Release) 1.4.0_01 & prior, 1.3.1_04 & prior, 1.3.0_05 & prior, 1.2.2_012 & prior	A vulnerability exists because the Sun Java Runtime Environment does not properly protect trusted java applets, which could let a remote malicious user obtain sensitive information.	Upgrades available at: http://java.sun.com/j2se/	SDK & JRE Access Control	Medium	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[164]	Unix	JRE (Linux Production Release) 1.4.1 _02	A vulnerability exists due to the way temporary files are generated, which could let a remote malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Java Virtual Machine Insecure Temporary File	Medium	Bug discussed in newsgroups and websites.

[163] Sun(sm) Alert Notification, 55100, June 4, 2003.
[164] Securiteam, June 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[165]	Unix	Solaris 8.0, 8.0_x86	A Denial of Service vulnerability exists in the syslog daemon when processing UDP packets.	Patches available at: http://sunsolve.sun.com/pub-cgi/	Solaris Syslogd UDP Packet Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[166]	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A remote Denial of Service vulnerability exists in the Telnet daemon.	Patches available at: http://sunsolve.sun.com	Solaris Telnet Daemon Remote Denial Of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[167]	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A buffer overflow vulnerability exists in the 'utmp_update' utility, which could let a malicious user obtain root privileges.	Patches available at: http://sunsolve.sun.com/pub-cgi/	Solaris 'UTMP_ Update' Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[168]	Unix	SunMC Change Manager 1.0	A buffer overflow vulnerability exists in the 'pamverifier' program, which could let a local/remote malicious user obtain root access.	Patches available at: http://sunsolve.sun.com Patch 113105-01 Patch 113106-01	Sun Management Center PamVerifier Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[165] SecurityFocus, June 5, 2003.
[166] Sun(sm) Alert Notification Sun Alert, 54181, June 2, 2003.
[167] Sun(sm) Alert Notification, 55260, June 5, 2003.
[168] Sun(sm) Alert Notification Sun Alert, 55160 May 30, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Microsystems, Inc.[169] ***Updates available*** [170]	**Windows 2000, XP**	**Sun One Application Server 7.0 Standard Edition, 7.0 Platform Edition**	**Multiple vulnerabilities exist: a vulnerability exists due the way the case of a file extension is handled, which could let a remote malicious user obtain sensitive information; a Cross-Site Scripting vulnerability exists due to insufficient filtering of script code from URL parameters, which could let a remote malicious user execute arbitrary code; a vulnerability exists because requests are not properly logged, which could let a remote malicious user obscure attacks from the view of administrators; and a vulnerability exists because the username and password for the administrative server is stored in a world-readable file during installation, which could let a remote malicious user obtain unauthorized access to the administrative server.**	***Upgrade available at:*** **http://wwws.sun.com/software/download/products**	**Sun ONE Application Server Multiple Vulnerabilities**	**Medium/ High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. File extension and log request vulnerabilities can be exploited via a web browser. Proof of Concept exploit has been published for the Cross-Site Scripting vulnerability. There is no exploit code required for the password storage vulnerability.**
Synkron. web[171]	Windows	Synkron. web 3.5, 3.0	A Cross-Site Scripting vulnerability exists in the search script due to insufficient sanitization of HTML code, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Synkron.Web Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
The XMB Group[172]	Multiple	Forum 1.8, SP1	Several vulnerabilities exist: a vulnerability exists when U2U private messages are viewed due to insufficient sanitization, which could let a malicious user execute arbitrary HTML code; and a vulnerability exists in the 'Location' field due to insufficient sanitization, which could let a malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	XMB Forum Code Execution	**High**	Bug discussed in newsgroups and websites.

[169] SPI Labs Advisory, May 27, 2003.
[170] SecurityFocus, June 4, 2003.
[171] Securiteam, June 9, 2003.
[172] SecurityFocus, June 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Webfroot[173]	Unix	Shoutbox 2.32 & prior	Several vulnerabilities exist: a Directory Traversal vulnerability exists due to insufficient sanitization of user-supplied values to URI parameters, which could let a malicious user obtain sensitive information; and a vulnerability exists in the 'conf' parameter, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Shoutbox Directory Traversal & Code Injection	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Webfroot[174]	Windows, Unix	Shoutbox 2.32	Several vulnerabilities exist in the 'expanded.php' script due to insufficient sanitization of user-supplied input, which could let a malicious user obtain sensitive information or execute arbitrary code.	No workaround or patch available at time of publishing.	Shoutbox Expanded.PHP Remote Command Execution	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.
WinMX[175]	Multiple	WinMX 2.6	A vulnerability exists because P2P passwords are stored in plaintext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WinMX Plaintext Password Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Word-Press[176]	Windows, Unix	WordPress 0.7	Several vulnerabilities exist: a vulnerability exists in the '/wp-links/links.all.php' script due to insufficient verification of the 'abspath' parameter, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the '/blog.header.php' script due to insufficient verification of the 'posts' parameter, which could let a remote malicious obtain administrative privileges.	No workaround or patch available at time of publishing.	WordPress 'abspath' & 'posts' parameters	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Xaos[177]	Unix	Xaos 3.0	A buffer overflow vulnerability exists in the command option processing, which could let a malicious user obtain root privileges.	**Debian:** http://security.debian.org/pool/updates/main/x/xaos/	Xaos Language Option Local Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[173] Securiteam, May 30, 2003.
[174] SecurityFocus, June 2, 2003.
[175] SecurityFocus, June 2, 2003.
[176] SecurityFocus, June 2, 2003.
[177] Debian Security Advisory, DSA 310-1, June 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Xinetd[178] ***Vendors issue advisories*** *[179, 180, 181]* ***More patches released*** *[182]*	**Unix**	**Xinetd 2.3-2.3.10**	**A remote Denial of Service vulnerability exists in the 'sve_request' function when connection attempts to some services are rejected.**	**Upgrade available at:** **http://www.xinetd.org/xinetd-2.3.11.tar.gz** ***RedHat:*** **ftp://updates.redhat.com** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***Sun:*** **http://sunsolve.sun.com/patches/linux/security.html** ***YellowDog:*** **ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/**	**Xinetd Remote Denial of Service** **CVE Name: CAN-2003-0211**	**Low**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Xinetd[183] ***Vendors issue advisories*** *[184, 185, 186]* ***More patches released*** *[187]*	**Unix**	**Xinetd 2.3-2.3.10**	**A remote Denial of Service vulnerability exists in the 'sve_request' function when connection attempts to some services are rejected.**	**Upgrade available at:** **http://www.xinetd.org/xinetd-2.3.11.tar.gz** ***RedHat:*** **ftp://updates.redhat.com** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***Sun:*** **http://sunsolve.sun.com/patches/linux/security.html** ***YellowDog:*** **ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/**	**Xinetd Remote Denial of Service** **CVE Name: CAN-2003-0211**	**Low**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Xmame[188]	Multiple	Xmame 0.62.1, 0.62.2, 0.66.1, 0.66.2, 0.67.1, 0.67.2, 0.68.1, 0.69.1	A buffer overflow vulnerability exists in the language setting (--lang) line parameter due to insufficient bounds checking, which could let a malicious user execute arbitrary instructions with elevated privileges.	No workaround or patch available at time of publishing.	Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[178] Bugtraq, April 18, 2003.
[179] Red Hat Security Advisory, RHSA-2003:160-01, May 13, 2003.
[180] Mandrake Linux Security Update Advisory, MDKSA-2003:056, May 14, 2003.
[181] Red Hat Security Advisory, RHSA-2003:161-07, May 22, 2003.
[182] Yellow Dog Linux Security Announcement, YDU-20030602-1, June 2, 2003.
[183] Bugtraq, April 18, 2003.
[184] Red Hat Security Advisory, RHSA-2003:160-01, May 13, 2003.
[185] Mandrake Linux Security Update Advisory, MDKSA-2003:056, May 14, 2003.
[186] Red Hat Security Advisory, RHSA-2003:161-07, May 22, 2003.
[187] Yellow Dog Linux Security Announcement, DU-20030602-1, June 2, 2003.
[188] Secunia Security Advisory, June 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Xpres-sions Interactive Inc.[189]	Multiple	eVision, Flower-Link, true-connect, Website Integration	Several vulnerabilities exist: a vulnerability exists in the 'login.asp' script due to insufficient validation, which could let a remote malicious user obtain administrative access; and a vulnerability exists because user information is stored in the database without encryption, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Xpressions Interactive 'login.asp' script & Information Disclosure	Medium/ **High** **(High if adminis-trative access can be obtained)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Zendocs[190]	Windows, Unix	zenTrack 2.2-2.2.2, 2.3-2.3.2, 2.4, 2.4 .1	Several vulnerabilities exist: a vulnerability exists in the 'index.php' script due to insufficient sanitization of user-supplied variables, which could let a remote malicious user execute arbitrary code; a vulnerability exists when debug mode is enabled, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in the 'translator.class' file in the '/test' directory, which could let a remote malicious user specify an alternate location for the libDir variable.	No workaround or patch available at time of publishing.	zenTrack Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Debug mode vulnerability can be exploited via a web browser. Proof of Concept exploit has been published for the 'index.php' vulnerability.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

[189] SecurityTracker Alert ID, 1006921, June 4, 2003.
[190] Bugtraq, June 6, 2003.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between May 30 and June 12, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 30 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
June 12, 2003	bazarr-episode-4.c	Script that exploits the Xaos Language Option Local Buffer Overflow vulnerability.
June 12, 2003	bazarr-unsencored-episode-3.c	Script that exploits the Eterm Buffer Overflow vulnerability.
June 11, 2003	redfang.tar.gz	Proof-of-concept application to find non discoverable bluetooth devices. This is done by brute forcing the last six (6) bytes of the bluetooth address of the device and doing a read_remote_name().
June 11, 2003	**Tripbit-AMSxpl.c**	**ArGoSoft Mail Server Remote Denial of Service vulnerability.**
June 10, 2003	aimcrack-0.1.tar.gz	Utility that brute-forces AIM screenames and passwords. In a list of about 1500 passwords, aimcrack takes about 2 hours on a cable modem connection
June 10, 2003	atftpdx.c	Script that exploits the ATFTPD Remote Filename Length Buffer Overrun vulnerability.
June 10, 2003	bufferpaper.txt	A document that goes into great detail describing how to utilize format string attacks with limited buffer space.
June 10, 2003	mencari_asal_usul.pl	Proof of concept exploit for the mnoGoSearch 'tmplt' Parameters Buffer Overflow vulnerability.
June 10, 2003	mencari_sebuah_nama.pl	Proof of concept exploit for the MNOGoSearch 'ul' & 'tmplt' Parameters Buffer Overflow vulnerabilities.
June 10, 2003	**mwmxploit.c**	**Script that exploits the Magic Winmail Remote Denial of Service vulnerability.**
June 10, 2003	x_diagrpt_aix5l_4x.sh	Script that exploits the AIX diagrpt Command vulnerability.
June 10, 2003	x_errpt_aix5.pl	Script that exploits the AIX errpt Command vulnerability.
June 10, 2003	**x_lsmcode_aix4x.pl**	**Script that exploits the AIX lsmcode Command vulnerability.**
June 9, 2003	**hp_rs.F3000.sh**	**Script that exploits the HP-UX rs.F3000 Unauthorized Access vulnerability.**
June 9, 2003	hp_stmkfont.c	Script that exploits the HP-UX 'stmkfont' Buffer Overflow vulnerability.
June 5, 2003	priv8kon.pl	Perl script that exploits the Multiple Vendor kon2 Buffer Overflow vulnerability.
June 5, 2003	**xxzb.c**	**Script that exploits the Zblast Buffer Overflow vulnerability.**
June 4, 2003	**ca-dbpwrecover.pl**	**Perl script that exploits the Unicenter Asset Manager Stored Data Decryption vulnerability.**
June 4, 2003	ie-object-ex.pl	Perl script that exploits the Microsoft Internet Explorer OBJECT Tag Buffer Overflow vulnerability.
June 3, 2003	THCsql.zip	Exploit for the MSSQL OpenDataSource function vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
June 3, 2003	**xmame_exploit.c**	**Script that exploits the XMame Buffer Overflow vulnerability.**
June 3, 2003	**xmanfmt.c**	**Script that exploits the Man Catalog File Format String vulnerability.**
June 2, 2003	**crobftp.asm**	**Exploit for the Crob FTP Server Remote Username Format String vulnerability.**
June 2, 2003	**expanded.pl**	**Perl script that exploits the Shoutbox Expanded.PHP Remote Command Execution vulnerability.**
June 2, 2003	pi3web_dos.c	Script that exploits the Pi3Web Buffer Overflow vulnerability.
May 30, 2003	**am2002_dos.c**	**Exploit for the Activity Monitor 2002 Remote Denial of Service vulnerability.**
May 30, 2003	amap-2.5.tar.gz	A scanning tool that allows you to identify the applications that are running on a specific port. It does this by connecting to the port(s) and sending trigger packets.
May 30, 2003	**jeritan_batinku.pl**	**Perl script that exploits the Shoutbox Directory Traversal & Code Injection vulnerabilities.**
May 30, 2003	ne0.c	Script that exploits the Microsoft IIS versions 5.0 and 5.1 Remote Denial of Service vulnerability.
May 30, 2003	nmapgrep.c	A tool that is customized to grep regular expression patterns from a nmap log file and output the IP addresses that match the pattern.

Trends

- **The Department of Homeland Security has noticed an increase in the use of mass mailing techniques to distribute malicious code. Several recent forms of malicious code, such as the W32/Fizzer@MM Worm (see DHS Advisory 03-#023), variations of the Sobig virus (W32/Sobig-A, B and C), and BugBear (W32/BugBear A and B) were propagated via e-mail. For more information see: http://www.nipc.gov/publications/infobulletins/2003/MassMailingMalicious%20Code.htm.**
- **The underlying code for the Slammer worm is planned to be published by *Wired* magazine. The article, which will be published in Wired's July issue due out on Tuesday, details how the Slammer worm, also known as "SQL Slammer," spread rapidly through the Internet on Jan. 25, shutting down Internet service providers in South Korea, disrupting plane schedules and knocking out automatic teller machines.**
- **A new version of the network worm "Sobig" has been detected, Sobig.c. There here have been numerous registered infections from the new version of this malicious program.**
- **Sobig.B (Aliases: Palyh or Mankx) infections have been reported from over 80 countries worldwide. This worm is spreading at an increasing pace. The largest infections seem to be in UK and USA. It spreads via e-mail attachments and Windows network shares. The e-mails sent by the worm pretend to come from support@microsoft.com and they contain the message text "All information is in the attached file." Windows users everywhere are urged to update their anti-virus definitions.**
- According to new research, nearly three-quarters of malicious connections to wireless networks are used for sending spam. A survey found that almost a quarter of unauthorized connections to the wireless LANs were intentional, and 71 per cent of those were used to send e-mails.
- **The Department of Homeland Security (DHS), Information Analysis and Infrastructure Protection (IAIP) has issued an advisory to heighten awareness of a recently discovered Snort(TM) vulnerability, a heap overflow in the Snort "stream4" preprocessor (CAN-2003-0029). For more information see 'Bugs, Holes, & Patches Table (CyberNotes 2003-08) and DHS/IAIP Advisory 03-018, located at: http://www.nipc.gov/warnings/advisories/2003/03-018.htm**

- **The number of security events detected by companies in the first quarter of 2003 jumped nearly 84 percent over the preceding three months. The increase in events, which can include minor probes for holes in network security as well as major attacks, stems mainly from an increase in worms and automated attack software.**
- Over the past few weeks, their have been an increased number of reports of intruder activity involving the exploitation of Null (i.e., non-existent) or weak Administrator passwords on Server Message Block (SMB) file shares used on systems running Windows 2000 or Windows XP. This activity has resulted in the successful compromise of thousands of systems, with home broadband users' systems being a prime target. Recent examples of such activity are the attack tools known as W32/Deloder, GT-bot, sdbot, and W32/Slackor. For more information, see CERT® Advisory CA-2003-08, located at: http://www.cert.org/advisories/CA-2003-08.html.

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

BAT_FORCA.C (Alias: IRC.Forca.Worm) (Batch File Form): This non-memory resident script worm usually arrives via an infected email. It also drops a Visual Basic Script (VBS) file to facilitate its mass-mailing routine and sends the worm to all target recipients listed in the Microsoft Outlook Address Book.

Bat.Mumu.A.Worm (Aliases: Worm.Win32.Muma, BAT.Muma, Bat/Mumu.worm, BAT.Mumu.A.Worm, BAT_SPYBOT.ABAT/Mumu.worm, Bat/Mumu-A, Muma, HackTool.Win32.Hucline) (Batch File Worm): This worm is a collection of batch files and utilities, as well as a hacktool named Hacktool.Hacline. It is possible that the names and functions of the files may change. It will spread using administrative shares on Windows NT, 2000, and XP systems. The worm will execute on the Windows 95/98/Me systems; however, it does not harm these systems.

Ircobus (Alias: Worm.Win32.Ircobus) (Win32 Worm): This script-based worm consists of a few mIRC scripts and batch files. It is spread in a self-extracting archive that beside the Ircobus worm drops DoS (Denial of Service) Trojans, a modified mIRC client that works with worm's scripts, and a few utilities including HideWindow (hides application windows) and PsExec (starts or kills processes on a remote computer). When the self-extracting archive is run by a user, it hides and drops a few files to \%winsysdir%\drivers\media\cat32\ folder. Then a startup key is created for the modified mIRC file so that it could be loaded during all Windows sessions. When the modified mIRC client is started, it loads a few scripts including the Ircobus worm script. The script looks for network shares with the help of external utilities, builds a list of vulnerable computers and then spreads to these computers by copying the dropper file to remote hard disks. The dropper is then activated with the help of PsExec.exe utility and a remote computer becomes infected.

JS/Fortnight.C (JavaScript Worm): This script worm drops URL links to the following locations:

- C:\Windows\favorites\nude nurses.url
- C:\Windows\favorites\search you trust.url
- C:\Windows\favorites\your favorite porn links.url

The content of the new .URL files is:

- %6F%6D>http://auto.search.msn.com:3128@%%6F%6D

Muma (Alias: Worm.Win32.Muma, HackTool.Win32.Hucline) (Win32 Worm): This network worm consists of a few batch scripts, a few utilities and a malicious user's tool called Hucline. It uses Hucline to scan for vulnerable computers and then it tries to connect to IPC$ share and to copy its files to Windows System folder of remote computers. After that the worm starts its main file on a remote computer and that computer becomes infected and spreads the worm further on.

PE_BUGBEAR.DAM (File Infector): This identification is for damaged samples of the mass-mailing virus, PE_BUGBEAR.B. Files infected with PE_BUGBEAR.DAM can no longer spread, run, and infect other executable files. This malware affects systems that run Windows 95, 98, NT, 2000, ME, and XP operating systems.

VBS.Purify@mm (Win32 Worm): This mass-mailing worm is written in Microsoft Visual Basic Script. It sends itself as an attachment to all the addresses in the Microsoft Outlook Address Book. The e-mail has the following characteristics:

- Subject: Something givin' has no value
- Attachment: Purify.vbs

W32.Bugbear.B@mm (Aliases: Win32.Bugbear.B, W32/Bugbear.b@MM, PE_BUGBEAR.B, W32/Bugbear-B, I-Worm.Tanatos.b, W32.Shamur, W32.Kijmo, Bugbear.B, W32/Bugbear.B, W32/Bugbear.b.dam Win32/Bugbear.B@mm, Worm/BugBear.B, W32/Kijmo.A-mm, W32/Bugbear.B@mm, W32/Kijmo.A, I-Worm.Tanatos.B) (Win32 Worm): This variant of W32.Bugbear@mm is a mass-mailing worm that also spreads through network shares. It is polymorphic and also infects a select list of executable files. It possesses keystroke-logging and backdoor capabilities, and attempts to terminate the processes of various antivirus and firewall programs. The worm uses the Incorrect MIME Header Can Cause IE to Execute E-mail Attachment vulnerability to cause unpatched systems to auto-execute the worm when reading or previewing an infected message. In addition, it contains routines that specifically affect financial institutions. This functionality will cause the worm to send sensitive data to one of ten hard-coded public Internet e-mail addresses. The information sent includes cached passwords and key-logging data. Because the worm does not properly handle the network resource types, it may flood shared printer resources, which causes them to print garbage or disrupt their normal functionality.

W32.Femot.Worm (Aliases: WORM_MOFEI.B, W32/MoFei.worm, WORM_MOFEI.A, W32/Mofei-A, Backdoor.Mofeir.101, Mofei, Backdoor.Mofeir.101, Mofeir, Worm.Win32.Mofeir) (Win32 Worm): This worm attempts to spread through a local network. The worm attempts to use ports 135 and 139. W32.Femot.Worm also has backdoor capabilities.

W32.HLLP.Kroter (Win32 Worm): This virus infects files in the folders that belong to popular file-sharing programs. This virus is written in Borland Delphi.

W32.HLLW.Aldem@mm (Win32 Worm): This mass-mailing worm attempts to spread itself through e-mail, mIRC, and across file-sharing networks. The worm also contains a backdoor functionality and attempts to terminate the processes of various programs, including antivirus and security software. The e-mail messages will have the following characteristics:

- Subject: Re:
- Attachment: melda.scr.

It is written in the Borland C++ programming language and is compressed with UPX.

W32.HLLW.BenfGame.B (Alias: Worm.Win32.Fasong.a) (Win32 Worm): This worm is written in the Delphi programming language. It has a password-stealing component and a worm component. The worm spreads to all the mapped and network-shared drives under an assortment of randomly generated filenames.

W32.HLLW.Cidas@mm (Aliases: I-Worm.Centar.h, W32/Fourseman.g@MM) (Win32 Worm): This mass-mailing worm attempts to spread itself through e-mail, mIRC, and file-sharing networks. The e-mail messages can have a variety of subjects and a variety of attachments. It is written in the Visual Basic and is compressed with UPX.

W32.HLLW.Lavits (Alias: W32.HLLW.Xolox@mm) (Win32 Worm): This worm attempts to spread across the KaZaA file-sharing network. It also uses Microsoft Outlook to send e-mail to all the contacts in the Microsoft Outlook Address Book. When run, it will display a fake message with the message title "Application Error." The e-mail does not have an attachment. The e-mail messages have the following characteristics:

- Subject: Where are you?

It is written in Visual Basic (VB) and is packed with UPX.

W32.HLLW.Lovgate.K@mm (Aliases: I-Worm.LovGate.i, W32/Lovgate.l@M) (Win32 Worm): This variant of W32.HLLW.Lovgate.I@mm has been repacked to make it difficult for existing antivirus software to detect. It is also a mass-mailing worm that attempts to e-mail itself to all the e-mail addresses it finds in the files whose extensions start with "ht." The subject and attachment of the incoming e-mail are chosen from a predetermined list. It attempts to copy itself to all the computers on a local network, and then infect those computers. The worm also has Backdoor Trojan capabilities. By default, the Trojan component listens on port 10168. If the infected computer runs Windows NT, 2000, or XP, the worm will attempt to disguise itself as the normal Windows process, "LSASS.EXE." This threat is written in the C++ programming language and is compressed several times with ASPack.

W32.HLLW.Nool@m (Win32 Worm): This worm attempts to spread itself through e-mail. The worm replies to the first e-mail it finds in Microsoft Outlook. The e-mail will have a variable subject and attachment name. The attachment will have a double extension, the last of which will be either .com, .exe, .pif, or .scr. The worm contains a backdoor capability and it attempts to connect to a specified IRC channel on port 6667. This threat is written in the Borland Delphi programming language.

W32.HLLW.Spirit (Win32 Worm): This worm spreads through the KaZaA file-sharing network. It copies itself as %Windir%\System32\Explorer.exe. The worm is written in the Microsoft Visual Basic programming language.

W32.Mapson.Worm (Alias: W32/Mapson-A, I-Worm.Mapson, W32/Mapson@MM, Lorraine, Mapson, I-Worm.Mapson) (Win32 Worm): This worm sends itself to all contacts found in the MSN messenger contact list. The Subject line, Message body, and attachment vary. The attachment will have a .com, .exe, or .pif file extension. The e-mail also may have spoofed 'From' field. The worm also attempts to spread itself through KaZaA, KaZaA Lite, eDonkey2000, Gnucleus, Limewire, Morpheus, Grokster file-sharing networks and ICQ. It is written in the Borland Delphi programming language and is compressed with UPX.

W32.Naco.C@mm (Alias: W32/Naco.d@MM) (Win32 Worm): This mass-mailing worm attempts to spread itself through the e-mail and file-sharing networks. The worm also contains backdoor functionality and attempts to replace HTML files on the Microsoft IIS server. The e-mail messages can have a variety of subjects and the following attachment:

- ANACON32.EXE

W32.Naco.D@mm (Alias: W32/Anacon-D) (Win32 Worm): This variant of W32.Naco@mm is a mass-mailing worm written in Visual Basic (VB). The worm can spread via e-mail, peer-to-peer file-sharing applications, such as KaZaA, as well as network shares. The worm also has the capability to run as a Backdoor Trojan Horse. It can also replace HTML files on Microsoft IIS servers.

W32.Randex.B (Win32 Worm): This network-aware worm that will copy itself to the following paths on computers with weak administrator passwords:

- \Admin$\system32\msslut32.exe
- \c$\winnt\system32\msslut32.exe

W32.Redzed@mm (Win32 Worm): This mass-mailing worm has password-stealing capabilities. The e-mail will have a variable subject line and attachment name chosen from a hard-code list. The attachment will have either a .exe or .pif file extension. This worm also spreads through various file-sharing networks.

W32.Supova.C.Worm (Alias: Worm.P2P.Surnova.c) (Win32 Worm): This worm attempts to spread through the KaZaA file-sharing network. This threat is written in the Microsoft Visual Basic (VB) programming language and is compressed with Petite. The VB run-time libraries are required to execute the worm. NOTE: Due to the bugs in the code, W32.SupoVirginiaC may not properly work.

W32/Backzat-K (Aliases: I-Worm.BatzBack.i, WORM_BACKZAT.A) (Win32 Worm): This worm spreads via mIRC, AIM95 and the KaZaA file-sharing network. Upon execution the worm copies itself as BatzBack.scr to the Windows and Windows System folders and sets the following registry entry with the path to the copy in the Windows folder:

- HKLM\Software\Microsoft\Windows\Current Version\Run\BatzBack

To spread through the KaZaA file-sharing network and AIM95 the worm attempts to copy itself as EnimEmSpearsBritney.scr and BuddyShare.exe to the KaZaA shared folder and Program Files\AIM95 respectively. To spread through IRC the worm modifies or creates script.ini so that Batzback.scr is sent to other users who join the current channel.

W32/HorseMan.B (Win32 Worm): W32/HorseMan.B is an Internet worm that spreads over e-mail by using addresses it collects in the Microsoft Outlook Address Book. The worm arrives through e-mail in the following format:

- Subject: A windows patch
- Attachment: Explorer.exe

If executed, the worm will first move the Explorer.exe file, C:\Windows\Explorer.exe to C:\Windows\Temp\Explorer.exe. Then, it will copy itself as Explorer.exe into the C:\Windows directory. The following registry key will get added:

- HKEY_LOCAL_MACHINE\Software\4HorseMan"MAPI"="Done"

W32/HorseMan.B will shut down various personal firewall and antivirus software applications, as well as, terminate the processes of some Windows files (e.g. Regedit.exe).

W32/Jeefo-A (Aliases: PE_JEEFO.A, W32/Jeefo, W32.Jeefo)(Win32 Worm): This worm may create the following registry entries upon execution, so that it is run every time the computer restarts:

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\PowerManager = "<full file path>"
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\PowerManager = "C:\<Windows>\SVCHOST.EXE"

W32/Outsider.C (Win32 Worm): This Internet worm spreads over e-mail by using addresses it collects in the Microsoft Outlook Address Book. The worm arrives through e-mail in the following format:

- Subject: Some card games
- Attachment: Card_install.pif

If executed, the worm copies itself in the following locations:

- C:\Windows\System\Winlg32.pif
- C:\Windows\Card_install.pif
- C:\Windows\Mslg32.exe

So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "SecureLogin"="C:\\WINDOWS\\Mslg32.exe"

The following key also gets added:

- HKEY_LOCAL_MACHINE\Software\Zed\Outsider\Outsider3]"W32/Outsider.C by Zed"=""

W95.Tenrobot.C (Alias: Win95.Tenrobot.C) (Word 95 Macro Virus): This is a memory-resident, file-appending virus. It is a variant of W95.Tenrobot. This virus only infects files when it is executed on a Windows 95/98/Me system. W95.Tenrobot.C also attempts to give its creator unauthorized access to an infected computer through IRC.

W97M.Radnet (Word 97 Macro Virus): This macro virus that infects Microsoft Word documents and templates. It performs varying actions such as disabling keyboard shortcuts, disabling macro virus protection and replacing words in the current document.

WORM_AURIC.B (Alias: W32/Magold-B) (Internet Worm): This mass-mailing worm propagates via email to all recipients it finds in the Windows Address Book and in all files with an *.ht* extension. The email message it sends out is in Hungarian and its characteristics are as follows:

- From: erotika@lap.hu
- Subject: Maya Gold-os kepernyokimelo!
- Attachment: Maya Gold.scr

This malware runs on Windows NT, 2000 and XP systems.

WORM_AURIC.C (Alias: W32/Magold-C) (Internet Worm): This mass-mailing worm propagates via email to all recipients it finds in the Windows Address Book and in all *.HT* files. The email message it sends out is in Hungarian and has the following details:

- From: erotika@lap.hu
- Subject: Maya Gold-os kepernyokimelo!
- Attachment: Maya Gold.scr

In addition, this worm also spreads via mIRC and through the following peer-to-peer programs: Bearshare, Edonkey2000, Gnucleus, Grokster, ICQ, Limewire, Morpheus, and Shareaza. This worm terminates different processes that can be antivirus products. It also does the following at random intervals:

- Opens the CD-ROM drive
- Fills the Desktop area with blank text files with the file name RAVE##.TXT, where ## is a counting number beginning from 1
- Changes the window color to red
- Prevents the mouse cursor from being moved to upper portions of the screen
- Writes the following message at the title area of opened windows: =:-) OFFSPRING is coOL =:-) PUNK'S NOT DEAD =:-)
- Opens the site www.offspring.com

This worm runs on Windows NT, 2000, and XP.

WORM_KIRBO.A (Aliases: Kirby, KirbyFlooder, W32/Kifie-D) (Win32 Worm): This worm propagates through known peer-to-peer applications, copies itself to mapped network drives, and through Internet Relay Chat (IRC). This worm's presence is indicated by the presence of the file CUTEKIRBY.SCR in the Windows system folder. This application runs in Windows 95, 98, 2000, NT, ME, and XP.

Worm/Naco.E (Alias: W32/Naco.d@MM, I-Worm.Nocana.e, W32/Naco.E@mm, Anacon, Nocana, Naco) (Internet Worm): This Internet worm spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book, as well as, spreading over the various peer-2-peer file sharing program like KaZaA, Morpheus and E-Donkey2000. It is written in the programming language Microsoft Visual Basic. The worm arrives through e-mail and can have a variety of subjects and one of the following attachments:

- chicky.exe
- junkbulk.exe
- seeker.exe
- NACO.exe
- naco.exe
- ANACON32.exe

If executed, the worm copies itself in the \windows\%systems% directory under filenames of the same name. It will also copy itself in the following locations so that it will be available for file exchanging through file-sharing programs:

- C:\Program Files\KMD\My Shared Folder\
- C:\Program Files\Kazaa\My Shared Folder\
- C:\Program Files\KaZaA Lite\My Shared Folder\
- C:\Program Files\Morpheus\My Shared Folder\
- C:\Program Files\Grokster\My Grokster\
- C:\Program Files\BearShare\Shared\
- C:\Program Files\Edonkey2000\Incoming\

- C:\Program Files\limewire\Shared\

So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "ALM"="%System%\ANACON32.EXE" "SysAnacon32"="%System%\SysAna32.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices "Services"="%System%\ANACON32.EXE"
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "Under20"="%System%\ANACON32.EXE"
- HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\Administrator "Startup"="%System%" "Enable"="Yes" "Parameters"="" "Path"="%System%\\SYSPOLY32.EXE"

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the CyberNotes-2003-12 of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
AdwareDropper-A	A	CyberNotes-2003-04
AIM-Canbot	N/A	CyberNotes-2003-07
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Amitis.B	B	CyberNotes-2003-11
Backdoor.AntiLam.20.K	K	CyberNotes-2003-10
Backdoor.Apdoor	**N/A**	**Current Issue**
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	F	CyberNotes-2003-09
Backdoor.Badcodor	**N/A**	**Current Issue**
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.Cli	Cli	CyberNotes-2003-10
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Bigfoot	N/A	CyberNotes-2003-09
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CamKing	N/A	CyberNotes-2003-10
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Cmjspy	N/A	CyberNotes-2003-10
Backdoor.CNK.A	A	CyberNotes-2003-10
Backdoor.CNK.A.Cli	Cli	CyberNotes-2003-10
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Cow	N/A	CyberNotes-2003-01

Trojan	Version	CyberNotes Issue #
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Death.Cli	Cli	CyberNotes-2003-10
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Delf.Cli	Cli	CyberNotes-2003-10
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dvldr	N/A	CyberNotes-2003-06
Backdoor.EggDrop	N/A	CyberNotes-2003-08
Backdoor.Fatroj	N/A	CyberNotes-2003-10
Backdoor.Fatroj.Cli	Cli	CyberNotes-2003-10
Backdoor.Fluxay	N/A	CyberNotes-2003-07
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.FTP_Ana.C	C	CyberNotes-2003-07
Backdoor.FTP_Ana.D	D	CyberNotes-2003-08
Backdoor.Fxdoor	N/A	CyberNotes-2003-10
Backdoor.Fxdoor.Cli	Cli	CyberNotes-2003-10
Backdoor.Graybird	N/A	CyberNotes-2003-07
Backdoor.Graybird.B	B	CyberNotes-2003-08
Backdoor.Graybird.C	C	CyberNotes-2003-08
Backdoor.Grobodor	**N/A**	**Current Issue**
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Comiz	N/A	CyberNotes-2003-11
Backdoor.IRC.Lampsy	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou.B	B	CyberNotes-2003-11
Backdoor.IRC.Ratsou.C	C	CyberNotes-2003-11
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.Kaitex.D	D	CyberNotes-2003-09
Backdoor.Kalasbot	N/A	CyberNotes-2003-09
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kol	N/A	CyberNotes-2003-06
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.LeGuardien.B	B	CyberNotes-2003-10
Backdoor.Litmus.203.c	c	CyberNotes-2003-09
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Marotob	N/A	CyberNotes-2003-06

Trojan	Version	CyberNotes Issue #
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.Mots	N/A	CyberNotes-2003-11
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	N/A	CyberNotes-2003-07
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	12.b	CyberNotes-2003-07
Backdoor.OptixPro.13	13	CyberNotes-2003-09
Backdoor.Peers	N/A	CyberNotes-2003-10
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	N/A	CyberNotes-2003-09
Backdoor.Pointex.B	B	CyberNotes-2003-09
Backdoor.Private	N/A	CyberNotes-2003-11
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Ratega	N/A	CyberNotes-2003-09
Backdoor.Recerv	N/A	CyberNotes-2003-09
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Rsbot	N/A	CyberNotes-2003-07
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	E	CyberNotes-2003-06
Backdoor.Sdbot.F	F	CyberNotes-2003-07
Backdoor.Sdbot.G	G	CyberNotes-2003-08
Backdoor.Sdbot.H	H	CyberNotes-2003-09
Backdoor.Sdbot.L	L	CyberNotes-2003-11
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	N/A	CyberNotes-2003-09
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Slao	N/A	CyberNotes-2003-11
Backdoor.Snami	N/A	CyberNotes-2003-10
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.Softshell	N/A	CyberNotes-2003-10
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.Syskbot	N/A	CyberNotes-2003-08

Trojan	Version	CyberNotes Issue #
Backdoor.SysXXX	N/A	CyberNotes-2003-06
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Tankedoor	N/A	CyberNotes-2003-07
Backdoor.Trynoma	N/A	CyberNotes-2003-08
Backdoor.Turkojan	N/A	CyberNotes-2003-07
Backdoor.Udps.10	1	CyberNotes-2003-03
Backdoor.UKS	N/A	CyberNotes-2003-11
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Winet	N/A	CyberNotes-2003-11
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdemon.126	126	CyberNotes-2003-10
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	ATG	CyberNotes-2003-09
BackDoor-AUP	N/A	CyberNotes-2003-11
BackDoor-AVF	**AVF**	**Current Issue**
BackDoor-AVH	**AVH**	**Current Issue**
BackDoor-AVO	**AVO**	**Current Issue**
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/CheckESP	**N/A**	**Current Issue**
BDS/Ciadoor.10	10	CyberNotes-2003-07
BDS/Evilbot.A	A	CyberNotes-2003-09
BDS/Evolut	N/A	CyberNotes-2003-03
BDS/PowerSpider.A	A	CyberNotes-2003-11
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
DoS-iFrameNet	N/A	CyberNotes-2003-04
Downloader.BO.B	B	CyberNotes-2003-10

Trojan	Version	CyberNotes Issue #
Downloader.BO.B.dr	B.dr	CyberNotes-2003-10
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	BW.c	CyberNotes-2003-07
Exploit-IISInjector	N/A	CyberNotes-2003-03
Gpix	N/A	CyberNotes-2003-08
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC/Flood.cd	cd	CyberNotes-2003-11
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Seeker.J	J	CyberNotes-2003-01
JS/Fortnight.c@M	c	CyberNotes-2003-11
JS/Seeker-C	C	CyberNotes-2003-04
JS/StartPage.dr	dr	CyberNotes-2003-11
JS_WEBLOG.A	A	CyberNotes-2003-05
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Kjie	**N/A**	**Current Issue**
Keylog-Perfect.dr	dr	CyberNotes-2003-09
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Keylog-Yeehah	**N/A**	**Current Issue**
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
MultiDropper-FD	N/A	CyberNotes-2003-01
Pac	N/A	CyberNotes-2003-04
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-AH	AH	CyberNotes-2003-08
ProcKill-Z	N/A	CyberNotes-2003-03
Proxy-Guzu	N/A	CyberNotes-2003-08
PWS-Aileen	N/A	CyberNotes-2003-04
PWSteal.ABCHlp	**N/A**	**Current Issue**
PWSteal.AlLight	N/A	CyberNotes-2003-01
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Kipper	N/A	CyberNotes-2003-10
PWSteal.Lemir.105	105	CyberNotes-2003-10
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	CyberNotes-2003-10

Trojan	Version	CyberNotes Issue #
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWSteal.Snatch	N/A	CyberNotes-2003-10
PWSteal.Sysrater	**N/A**	**Current Issue**
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-Watsn	N/A	CyberNotes-2003-10
PWS-WMPatch	N/A	CyberNotes-2003-07
PWS-Yipper	N/A	CyberNotes-2003-10
QDel359	359	CyberNotes-2003-01
QDel373	373	CyberNotes-2003-06
Qdel374	374	CyberNotes-2003-06
Qdel375	375	CyberNotes-2003-06
Qdel376	376	CyberNotes-2003-07
QDel378	378	CyberNotes-2003-08
QDel379	369	CyberNotes-2003-09
QDial6	6	CyberNotes-2003-11
Renamer.c	N/A	CyberNotes-2003-03
Reom.Trojan	N/A	CyberNotes-2003-08
StartPage-G	G	CyberNotes-2003-06
Stoplete	N/A	CyberNotes-2003-06
Swizzor	N/A	CyberNotes-2003-07
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	21	CyberNotes-2003-07
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
Tr/SpBit.A	A	CyberNotes-2003-04
Tr/VB.t	T	CyberNotes-2003-11
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Dloader-BO	BO	CyberNotes-2003-02
Troj/IRCBot-C	C	CyberNotes-2003-11
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Peido-B	B	CyberNotes-2003-10
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02

Trojan	Version	CyberNotes Issue #
Trojan.Kaht	N/A	CyberNotes-2003-10
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	CyberNotes-2003-10
Trojan.Myet	**N/A**	**Current Issue**
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.PopSpy	N/A	CyberNotes-2003-11
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Sidea	**N/A**	**Current Issue**
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.ExitWin	**N/A**	**Current Issue**
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS.Zizarn	N/A	CyberNotes-2003-09
VBS/Fourcourse	N/A	CyberNotes-2003-06
W32.Adclicker.C.Trojan	C	CyberNotes-2003-09
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Noops.Trojan	N/A	CyberNotes-2003-09
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Systentry.Trojan	N/A	CyberNotes-2003-03
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04
Xin	N/A	CyberNotes-2003-03

Backdoor.Apdoor (Aliases: CoreFlood, Backdoor.Apdoor.b): This backdoor Trojan is similar to Backdoor.Coreflood. It allows unauthorized remote access to the system on that it is running, and supports commands to modify registry settings, transfer files, and start or end processes. A sign of possible infection is the existence of two files in the %system% directory of the form:

- ABCDEFG.exe (28160 bytes)
- ABCDEFG.dll (69632 bytes).

The actual filenames used by the Trojan are random.

Backdoor.Badcodor (Alias: Backdoor.Badcodor.b): This Backdoor Trojan Horse gives its creator full control over your computer. The existence of the file Los.exe or Msdosdll.exe is an indication of a possible infection. Backdoor.Badcodor also contains keylogger capabilities.

Backdoor.Grobodor (Alias: Backdoor.Grobodor.406): This Backdoor Trojan Horse gives its creator unauthorized access to your computer. It opens port 31332, by default. This Trojan is written in the Delphi programming language and is packed with UPX.

BackDoor-AVF: This detection for a Trojan opens port TCP 80 (HTTP) on the victim machine. Incoming requests on that port are redirected to website in the Internet. After execution, the Trojan copies itself as SYS64.EXE into %WINDIR%\SYSTEM32. The worm creates a registry run key to load itself at system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Tuneling" = SYS64.EXE

It runs HTTP server on port TCP80 and redirects incoming requests to http://promin.*OMITTED*.gs. It also sends on start a notification to the IP address 66.220.17.33 containing information about the victim.

BackDoor-AVH: This remote access Trojan opens TCP Port 8583 and sends e-mail notification to the author, via ICQ mail. This e-mail message contains the following information: Victim IP Address; Port User\Pass (to access the Trojan server); ServerName; WinVer; ComputerName. The Trojan allows remote users to perform file operations, such as:

- Upload\Download files
- Create\Delete\Rename directories
- Delete\Rename files
- Execute programs

The Trojan copies itself to the WINDOWS (%WinDir%) directory and creates a registry run key to load itself at system startup:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Run "net" = C:\WINNT\net.exe

It creates an additional key value as well:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components net "StubPath" = C:\WINNT\net.exe ASC

BackDoor-AVO: This detection is for a remote access Trojan written in MSVC thought to originate from Japan. When run on the victim machine, the Trojan installs itself into the Windows directory as WMGR32.EXE, for example:

- C:\WINDOWS\WMGR32.EXE

A Registry key is added to run the Trojan at system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "wmgr32" = C:\WINDOWS\WMGR32.EXE

It also drops another file into the Windows directory, HGET.EXE (4,608 bytes). This component is used to download data from remote servers (via HTTP). It is detected as application Tool-HGet with the specified DATs, with application-type detections enabled. Port 8999 is opened on the victim machine through which the malicious user is able to connect to the backdoor. Notification of the compromised system is sent to the malicious user via HTTP, using a script library. The Trojan contains the string:

- Mogura server version1.00 build1

BDS/CheckESP (Alias: Backdoor.Checkesp, Troj/Tunnel-A): This Backdoor Trojan would potentially allow someone with malicious intent backdoor access to your computer. If executed, the Trojan adds the following file to the \windows\%system% directory, "Sys64.exe." So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "tunelling"="sys64.exe"

BDS/CheckESP was originally received as "Sys64.exe." By default, it listens on port 666.

Keylog-Kjie: This detection is for a keylogging Trojan written in MSVC. The Trojan carries two DLLs in its resources required for logging keystrokes and dispatching logs via SMTP. When the Trojan is run on the victim machine, it installs the following files to the Windows directory:

- %WinDir%\KJLIB.DLL (5,632 bytes) %WinDir%\KJPOST.DLL (7,168 bytes) %WinDir%\WINLDR32.EXE (20,480 bytes - copy of the Trojan)

The following directory is created in the system temporary directory:

- _KJTMPXXXP

Keystroke logs are written to this directory. Strings within the Trojan suggest it use the system default SMTP server for mailing out logs, although this was not observed in testing. The default SMTP server is determined from values within the following Registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Account Manager\Accounts

Keylog-Yeehah: This keylogging Trojan simply captures Window titles and typed keystrokes when run. This information is saved to a file mem.log in the WINDOWS (%WinDir%) directory. Periodically, an executable named KLM.EXE (this may change in future variants) is run. KLM.EXE simply mails the MEM.LOG file to a YAHOO.COM e-mail address, via the smtp server hq.ilo.ch. This Trojan does not copy itself to any locations, or create and registry or ini run keys.

PWSteal.ABCHlp (Aliases: Trojan.Win32.Abced, BackDoor-AKM): This password-stealing, Backdoor Trojan Horse attempts to send password information from a compromised computer to an address in China. By default it makes use of ports 1025 and 1027.

PWSteal.Sysrater (Alias: Trojan.PSW.Sysrater.q): This a password-stealer sends password information from a compromised computer to the Trojan's creator.

Trojan.Myet: This Trojan Horse makes changes to the computer settings in the registry. The existence of the file haha.exe is an indication of a possible infection. This Trojan does not have a damaging payload.

Trojan.Sidea (Aliases: Trojan.Spy.Recerv, Sidea): This Trojan Horse steals information and sends it to a malicious user by e-mail. It is written in Microsoft Visual C++.

VBS.ExitWin (Alias: VBS.Nordog): This Trojan horse is written in Microsoft Visual Basic. When it is run, the script asks a series of questions in Malay. If you enter the "wrong" answer, the script closes Windows.